KORPORATIV TARMOQLARDA ARP SPOOFING HUJUMLARINI ANIQLASH VA OLDINI OLISH

Qo‘yliyev Behro‘z Sherzod o‘g‘li
Xayriddinov Shaxboz Shavkatovich
Normamatov Xusan Baxodir o‘g‘li
Seytmamatov Sohibjon Muzaffar o‘g‘li
TATU, Kiberxavfsizlik fakulteti talabalari

Annotatsiya: *Korporativ tarmoqlarda axborot almashinuvi jarayonida ARP (Address Resolution Protocol) protokoli muhim rol o‘ynaydi. Ushbu protokol IP manzillarni MAC manzillarga moslashtirish uchun xizmat qiladi. Biroq ARP protokolida autentifikatsiya mexanizmining mavjud emasligi uni turli kiberhujumlarga, xususan ARP spoofing va ARP poisoning hujumlariga zaif qiladi. Mazkur hujumlar natijasida hujumchi tarmoq trafiklarini ushlab qolishi, foydalanuvchi ma’lumotlarini o‘g‘irlashi yoki “Man-in-the-Middle” hujumlarini amalga oshirishi mumkin.*

Kalit so‘zlar*: ARP spoofing, ARP poisoning, Man-in-the-Middle, kiberxavfsizlik, intrusion detection, korporativ tarmoq, network security, Ethernet.*

Hozirgi kunda korporativ tarmoqlar tashkilotlar faoliyatining asosiy infratuzilmalaridan biri hisoblanadi. Tarmoq texnologiyalarining rivojlanishi ma’lumot almashinuvi tezligini oshirgan bo‘lsa-da, kiberxavfsizlik bilan bog‘liq muammolarni ham keskin kuchaytirdi. Lokal tarmoqlarda keng qo‘llaniladigan ARP protokoli xavfsizlik nuqtai nazaridan zaif hisoblanadi.

ARP protokoli IP manzillarni fizik MAC manzillarga moslashtirish uchun ishlatiladi. Ushbu protokolning asosiy muammosi shundaki, u paketlarning haqiqiyligini tekshirmaydi. Shu sababli hujumchi soxta ARP javoblari yuborish orqali tarmoq qurilmalarining ARP jadvallarini o‘zgartirishi mumkin. Natijada tarmoq trafiklari hujumchi qurilmasi orqali o‘tadi.

ARP spoofing hujumlari bugungi kunda eng xavfli lokal tarmoq hujumlaridan biri hisoblanadi. Ushbu hujumlar ma’lumotlarni o‘g‘irlash, trafikni o‘zgartirish, sessiyalarni egallash va xizmatlarni izdan chiqarishga olib kelishi mumkin. Shu sababli ARP spoofing hujumlarini aniqlash va oldini olish zamonaviy tarmoq xavfsizligining muhim vazifalaridan biridir.

ARP protokoli va uning ishlash prinsipi

ARP — Address Resolution Protocol — lokal tarmoq ichida IP manzilga mos MAC manzilni aniqlash uchun xizmat qiladi. Qurilma ma’lum IP manzilga ega host bilan bog‘lanmoqchi bo‘lsa, avval ARP request yuboradi. Tarmoqdagi kerakli qurilma esa ARP reply orqali o‘z MAC manzilini yuboradi.

ARP ishlash jarayoni quyidagicha:

1. Qurilma maqsad IP manzilni aniqlaydi.
2. ARP request broadcast paket yuboriladi.

3. Tegishli host ARP reply qaytaradi.
4. MAC manzil ARP jadvaliga yoziladi.
5. Aloqa boshlanadi.

ARP protokolining asosiy kamchiligi autentifikatsiyaning mavjud emasligidir. Har qanday qurilma soxta ARP javob yuborishi mumkin.

ARP spoofing hujumining mohiyati

ARP spoofing — hujumchi tomonidan tarmoqdagi qurilmalarga soxta ARP paketlar yuborish orqali ARP jadvalini noto‘g‘ri ma’lumot bilan to‘ldirish jarayonidir.

Hujumchi o‘z MAC manzilini gateway yoki boshqa host IP manzili bilan bog‘laydi. Natijada foydalanuvchi trafiklari hujumchi orqali o‘tadi.

ARP spoofing natijasida quyidagi hujumlar amalga oshirilishi mumkin:

Hujum turi	Tavsifi
Man-in-the-Middle	Trafikni ushlab qolish
Session Hijacking	Sessiyani egallab olish
Packet Sniffing	Paketlarni kuzatish
DoS Attack	Xizmatni izdan chiqarish
Data Manipulation	Ma’lumotlarni o‘zgartirish

ARP spoofing hujumining ishlash mexanizmi

Hujumchi lokal tarmoqqa ulanganidan so‘ng soxta ARP reply paketlarini yuboradi. Ushbu paketlarda gateway IP manzili hujumchining MAC manzili bilan bog‘lanadi.

Jarayon quyidagicha amalga oshadi:

1. Hujumchi tarmoqni skanerdan o‘tkazadi.
2. Gateway va target host aniqlanadi.
3. Soxta ARP reply paketlari yuboriladi.
4. Qurilmalar ARP jadvallarini yangilaydi.
5. Trafik hujumchi orqali o‘tadi.

IPgateway→MACattackerIP_{gateway}

\rightarrow MAC_{attacker}IPgateway→MACattacker

Natijada foydalanuvchi gateway MAC manzili o‘rniga hujumchi MAC manzilidan foydalanadi.

ARP spoofing hujumlarini amalga oshirish vositalari

ARP spoofing hujumlari uchun turli vositalar mavjud:

Vosita	Vazifasi
Ettercap	MITM hujumlari
Cain & Abel	Trafik sniffing
Bettercap	Tarmoq ekspluatatsiyasi
Wireshark	Paketlarni tahlil qilish
Arpspoof	Soxta ARP paket yuborish

Mazkur vositalar tarmoq trafiklarini kuzatish va paketlarni modifikatsiya qilish imkonini beradi.

ARP spoofing hujumlarini aniqlash usullari

ARP spoofing hujumlarini aniqlash uchun quyidagi metodlardan foydalaniladi:

ARP jadval monitoringi

ARP jadvalidagi MAC manzillar o‘zgarishi doimiy kuzatiladi. Bir IP manzil uchun bir nechta MAC manzil aniqlansa shubhali holat yuzaga keladi.

Intrusion Detection System

IDS tizimlari anomal ARP trafiklarini aniqlaydi va administratorga ogohlantirish yuboradi.

Paket tahlili

Wireshark kabi vositalar yordamida ARP trafiklari monitoring qilinadi.

Network Behavior Analysis

Tarmoqdagi g‘ayritabiiy trafik oqimlari tahlil qilinadi.

ARP spoofing hujumlaridan himoyalanish usullari

Static ARP

Muhim qurilmalar uchun statik ARP yozuvlari kiritiladi. Bu ARP jadvalining avtomatik o‘zgarishini oldini oladi.

Afzalliklari:

- yuqori xavfsizlik;
- spoofing ehtimoli kamayadi.

Kamchiliklari:

- katta tarmoqlarda boshqarish qiyin.

Dynamic ARP Inspection

Dynamic ARP Inspection switch darajasida ARP paketlarni tekshiradi va soxta paketlarni bloklaydi.

DAI ishlash prinsipi:

1. Switch ARP paketni qabul qiladi.
2. DHCP Snooping jadvali bilan solishtiradi.
3. Noto‘g‘ri paketlar bloklanadi.

Dynamic ARP Inspection korporativ tarmoqlarda eng samarali himoya vositalaridan biri hisoblanadi.

VLAN segmentatsiyasi

Tarmoqni VLANlarga bo‘lish hujumlar tarqalishini cheklaydi.

Afzalliklari:

- xavfsizlik oshadi;
- broadcast trafik kamayadi;
- segmentatsiya hosil bo‘ladi.

Port Security

Switch portlariga faqat ma’lum MAC manzillarni biriktirish orqali ruxsatsiz qurilmalar bloklanadi.

Taklif etilayotgan himoya modeli

Mazkur tadqiqotda ARP spoofing hujumlariga qarshi ko‘p qatlamli himoya modeli taklif etiladi.

Himoya qatlami	Vazifasi
Network Segmentation	VLAN asosida ajratish

Dynamic ARP Inspection	Soxta ARP paketlarni aniqlash
IDS/IPS Systems	Anomaliyalarni aniqlash
Firewall Integration	Trafikni filtrlash
Real-Time Monitoring	Doimiy nazorat

Taklif etilgan model kompleks xavfsizlikni ta’minlaydi hamda MITM hujumlari xavfini kamaytiradi.

Himoya usullarining samaradorligi

Himoya usuli	Samaradorlik	Xarajat	Murakkablik
Static ARP	Yuqori	Past	Yuqori
DAI	Juda yuqori	O‘rta	O‘rta
VLAN	O‘rta	Past	Past
IDS/IPS	Yuqori	Yuqori	Yuqori
Port Security	O‘rta	Past	Past

Jadval natijalariga ko‘ra, Dynamic ARP Inspection va IDS/IPS tizimlari eng samarali himoya mexanizmlari hisoblanadi.

XULOSA

ARP spoofing hujumlari korporativ tarmoqlar uchun jiddiy xavf hisoblanadi. ARP protokolida autentifikatsiya mexanizmining mavjud emasligi ushbu hujumlarni amalga oshirishni osonlashtiradi. Hujumchilar MITM, sniffing va session hijacking kabi tahdidlarni amalga oshirish uchun ARP spoofing texnikasidan foydalanadi.

Tadqiqot davomida ARP spoofing hujumlarini aniqlash va oldini olish usullari tahlil qilindi. Natijalar Dynamic ARP Inspection, IDS/IPS tizimlari va VLAN segmentatsiyasi kompleks tarzda qo‘llanilganda eng samarali himoyani ta’minlashini ko‘rsatdi. Kelgusida sun’iy intellekt asosidagi intrusion detection tizimlarini ARP spoofing himoyasiga integratsiya qilish tarmoq xavfsizligini yanada kuchaytirishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. William Stallings. Network Security Essentials. Pearson Education, 2017.
2. Behrouz Forouzan. Data Communications and Networking. McGraw-Hill, 2013.
3. Eric Cole. Network Security Bible. Wiley Publishing, 2011.
4. Scarfone K. Guide to Intrusion Detection and Prevention Systems. NIST, 2012.
5. Omar Santos. Cisco Cybersecurity Operations Fundamentals. Cisco Press, 2018.
6. RFC 826 – Address Resolution Protocol.
7. OWASP Network Attack Reports.
8. IEEE Research on ARP Spoofing Detection Systems.