SIMSIZ TARMOQLARDA SUQILIB KIRISHGA ASOSLANGAN HUJUM VOSITALARINING TAHLILI

Jabbarov Nuriddin Akbarovich
Toshkent axborot texnologiyalari universiteti, assistent
nuriddinjabbarov2606@gmail.com
Jabborov Abdulla Akbar o‘g‘li
Toshkent axborot texnologiyalari universiteti Samarqand filiali, talaba
abdullajabborov3@gmail.com

Annotatsiya. Mazkur tezisda simsiz tarmoqlarda keng tarqalgan xavfsizlik tahdidi — suqilib kirish hujumlari va ularni amalga oshirishda foydalaniladigan dasturiy vositalar tahlil qilinadi. Suqilib kirish hujumlari natijasida hujumchi tarmoqqa ruxsatsiz kirib, foydalanuvchilarning shaxsiy ma’lumotlarini qo‘lga kiritishi, xizmatlarni ishdan chiqarishi yoki tarmoq ustidan nazoratni egallashi mumkin. Tadqiqot davomida Wireshark, Tcpdump, Aircrack-ng, Hashcat, Fluxion, Wifiphisher, MDK3/MDK4, Scapy kabi mashhur vositalarning ishlash printsiplari, hujum turlari, xavf darajasi va foydalanish imkoniyatlari o‘rganildi. Shuningdek, simsiz tarmoqlarda himoyani kuchaytirish uchun WPA3 shifrlash protokoli, MAC manzil filtratsiyasi, SSID yashirish, WIDS tizimlari va zaifliklarni audit qilish kabi samarali chora-tadbirlar tavsiya etildi. Tezis amaliy ko‘rsatmalar, skrinshotlar va jadval asosida hujum vositalarining imkoniyatlarini aniq tahlil qilishga qaratilgan bo‘lib, zamonaviy simsiz tarmoq xavfsizligini ta’minlash yo‘llarini aniqlashga xizmat qiladi.

Kalit so‘zlar: simsiz tarmoqlar, suqilib kirish, tarmoq xavfsizligi, sniffing, parolni buzish, soxta access point, DoS hujumlari, WPA/WPA2, tarmoq monitoringi, Aircrack-ng, Hashcat.

Abstract. This thesis analyzes one of the most significant security threats in wireless networks — intrusion-based attacks — and the software tools commonly used to carry them out. Such attacks allow unauthorized access to a network, enabling attackers to intercept users’ personal data, disrupt services, or gain control over network resources. The study examines the working principles, attack types, risk levels, and usability of popular tools such as Wireshark, Tcpdump, Aircrack-ng, Hashcat, Fluxion, Wifiphisher, MDK3/MDK4, and Scapy. In addition, effective protective measures against wireless threats are proposed, including the use of WPA3 encryption protocol, MAC address filtering, SSID hiding, Wireless Intrusion Detection Systems (WIDS), and vulnerability auditing. The thesis provides practical demonstrations, screenshots, and a comparative table to assess the technical capabilities of attack tools, contributing to the identification of modern methods for securing wireless networks.

Keywords: wireless networks, intrusion, network security, sniffing, password cracking, fake access point, DoS attacks, WPA/WPA2, network monitoring, Aircrack-ng, Hashcat.

KIRISH

Simsiz tarmoqlardagi xavfsizlik tahdidlarining eng muhim shakllaridan biri suqilib kirish hujumlaridir. Bunday hujumlar natijasida hujumchi tarmoqqa noqonuniy kirib, foydalanuvchilarning shaxsiy ma’lumotlarini o‘zlashtirishi, xizmatni to‘xtatishi yoki tarmoq resurslarini nazorat qilishi mumkin. Suqilib kirish hujumlari turli usullar va vositalar yordamida amalga oshiriladi. Ushbu bo‘limda simsiz tarmoqlarga qaratilgan suqilib kirish vositalari, ularning turlari, ishlash printsiplari hamda xavfsizlikka ta’siri o‘rganiladi.

Simsiz tarmoqlarga yo‘naltirilgan hujum vositalari quyidagi asosiy kategoriyalarga bo‘linadi.

Tarmoq monitoringi va sniffing vositalari — ushbu vositalar tarmoq trafigini kuzatish va foydalanuvchi ma’lumotlarini (masalan, parollar, identifikatorlar) ushlab qolish uchun xizmat qiladi. Shu jumladan:

Wireshark — ochiq kodli tarmoq protokoli tahlilchisi bo‘lib, 802.11 simsiz protokoli asosida kelayotgan trafikni batafsil ko‘rib chiqishga imkon beradi.

Tcpdump — buyruq qatori yordamida ishlaydigan kuchli sniffer bo‘lib, real vaqtda trafikni yozib olishga imkon yaratadi.

Parolni sindirish va autentifikatsiyani aylanib o‘tish vositalari — bu vositalar tarmoqqa kirish uchun zarur bo‘lgan WEP, WPA yoki WPA2 himoyalari ostidagi parollarni buzishga mo‘ljallangan:

Aircrack-ng — WEP va WPA-PSK parollarini sindirishda keng qo‘llaniladigan kuchli dasturiy ta’minot majmuasi.

Hashcat — GPU kuchidan foydalanib xeshlarni yuqori tezlikda buzishga mo‘ljallangan dastur. U asosan WPA/WPA2-PSK xeshlarini dictionary yoki brute-force usuli bilan sindirishda keng qo‘llaniladi.

Soxta kirish nuqtasi (Fake Access Point) yaratish vositalari — hujumchilar foydalanuvchilarni aldash uchun soxta AP yaratib, ularning trafikini nazorat qilish imkoniyatini beradi:

Fluxion — foydalanuvchini soxta login sahifasiga yo‘naltirib, parolni kiritishga majburlaydi.

Wifiphisher — haqiqiy tarmoqdan foydalanuvchilarni uzib, ularni soxta tarmoq orqali phishing sahifasiga yuboradi.

Denial of Service (DoS) va Deauthentication hujumlari uchun vositalar — bu vositalar yordamida hujumchi qurilmani APdan uzib qo‘yishi yoki tarmoq xizmatini to‘xtatishi mumkin:

MDK3/MDK4 — turli sinov hujumlarini amalga oshirish uchun mo‘ljallangan

dastur bo‘lib, kanalni to‘ldirish, beacon flooding va autentifikatsiya DoS kabi funksiyalarni bajaradi.

Scapy — foydalanuvchi tomonidan yozilgan maxsus paketlar yordamida deauthentication yoki spoofing hujumlarini amalga oshirish imkonini beradi.

Simsiz hujumlarning ishlash prinsipi. Hujumchi avvalo simsiz tarmoqdagi ochiq yoki zaif kirish nuqtalarini aniqlaydi. Keyin u tarmoqdagi trafikni kuzatib boradi (sniffing), maqsadli qurilmaning MAC manzilini aniqlaydi va signal kuchini o‘lchaydi. Shundan so‘ng, u soxta kirish nuqtasi (fake access point) yaratishi yoki qurilmalarni deauthentication hujumi orqali tarmoqdan uzib qo‘yishi mumkin.

Bu jarayonlardan so‘ng, foydalanuvchini aldab, haqiqiy parolni kiritishga majburlash yoki hujumchining qurilmasi orqali internetga ulanadigan qilib qurilmani boshqarish amalga oshiriladi.

MUHOKAMA VA NATIJALAR

Hozirgi kunda ko‘plab hujum vositalari ochiq manbali va bepul taqdim etiladi, shuningdek, ularni ishlatish uchun katta texnik bilim talab qilinmaydi. Bu esa xavf darajasini yanada oshiradi. Jumladan, WPA2 PSK bilan himoyalangan tarmoqlar ham dictionary attack yoki handshake usullari yordamida buzilishi mumkin.

Hujum vositalarining xavf darajasi ularning funksiyalari, qamrovi va aniqlik darajasiga bog‘liq bo‘ladi.

- Wireshark va Tcpdump – tarmoq trafigini kuzatish va zaifliklarni aniqlash uchun ishlatiladi.
- Aircrack-ng va Hashcat – parollarni to‘g‘ridan-to‘g‘ri buzishga mo‘ljallangan.
- Fluxion va Wifiphisher – foydalanuvchilarni aldash orqali parollarni qo‘lga kiritadi.
- MDK4 va Scapy – tarmoq faoliyatini to‘xtatish yoki xizmat rad etish (DoS) hujumlarini amalga oshiradi.

1-jadval

Hujum vositalarining texnik imkoniyatlari

Vosita nomi	Asosiy maqsadi	Hujum turi	Xavf darajasi	Foydalanuvchanligi
Aircrack-ng	WEP/WPA parollarini sindirish	Brute-force / Dictionary	Yuqori	Oson (CLI asosida)
Wireshark	Tarmoq trafikini tahlil qilish	Sniffing / Monitoring	O‘rta	Oson (GUI interfeys)
Wifiphisher	Soxta AP yaratish, phishing orqali parol olish	Social engineering (aldov)	Yuqori	O‘rta (sozlash kerak)
MDK3/MDK4	DoS, Beacon flooding	Tarmoqni ishdan chiqarish (DoS)	Yuqori	Oson (CLI)

Kismet	Passiv monitoring, SSID va qurilmalarni aniqlash	Passiv tahlil	Past	O‘rta
Reaver	WPS PIN orqali WPA2 buzish	WPS brute-force	Yuqori	Cheklangan (faqat WPS)

Simsiz tarmoqlarda xavfsizlik tahdidlariga qarshi samarali himoya choralarini ko‘rish zamonaviy axborot infratuzilmasining barqarorligi va maxfiyligini ta’minlashda muhim ahamiyatga ega. Tarmoq resurslariga ruxsatsiz kirishni, ma’lumotlar oqimini tahlil qilishni hamda turli xil hujumlarni oldini olish maqsadida quyidagi texnik va tashkiliy chora-tadbirlarni amalga oshirish tavsiya etiladi:

Zamonaviy shifrlash algoritmlaridan foydalanish simsiz tarmoqlar orqali uzatilayotgan ma’lumotlarning maxfiyligini ta’minlash uchun muhimdir. Masalan, WPA3 (Wi-Fi Protected Access 3) kabi ilg‘or shifrlash protokollari Simultaneous Authentication of Equals (SAE) texnologiyasiga tayangan holda, bruteforce va lug‘at hujumlariga qarshi yuqori darajadagi himoyani taqdim etadi. Ushbu algoritm foydalanuvchi parolini shifrlashda qo‘shimcha murakkab matematik usullarni qo‘llaydi, bu esa parolning o‘g‘irlanishini ancha qiyinlashtiradi.

MAC manzil filtratsiyasi va SSID uzatishni o‘chirish orqali tarmoqqa faqat maxsus ruxsat berilgan qurilmalar ulanishi ta’minlanadi, bu esa begona foydalanuvchilarning kirishini kamaytiradi. MAC manzillarga asoslangan filtratsiya tarmoq xavfsizligini oshiradi, SSIDning ommaviy uzatilishini o‘chirish esa potentsial hujumchilarga tarmoqni aniqlash imkoniyatini kamaytiradi.

Tarmoqni doimiy monitoring qilish va soxta kirish nuqtalarini aniqlash uchun maxsus vositalardan foydalanish zarur. Masalan, Wireless Intrusion Detection System (WIDS) tizimlari Wi-Fi muhitini real vaqt rejimida kuzatib boradi, nolegal (ruxsatsiz) access pointlarni aniqlaydi va “Evil Twin” hamda MITM hujumlari haqida administratorni darhol xabardor qiladi. Bu usul tarmoq xavfsizligini sezilarli darajada oshiradi.

Zaifliklarni baholash va audit o‘tkazish simsiz tarmoq xavfsizligini ta’minlashda muhim bosqich hisoblanadi. Buning uchun Nessus, NetSpot yoki Acrylic WiFi kabi vositalardan foydalaniladi. Ushbu dasturlar yordamida tarmoq topologiyasi, signal kuchi, autentifikatsiya mexanizmlari va shifrlash darajalari batafsil tahlil qilinadi. Natijada aniqlangan zaifliklar va kamchiliklar muntazam ravishda aniqlanib, tarmoq xavfsizligini oshirishga xizmat qiladi.

XULOSA

Simsiz tarmoqlar axborot almashinuvi va mobil aloqaning ajralmas qismiga aylangan hozirgi davrda ularning xavfsizligini ta’minlash dolzarb masala hisoblanadi. Ushbu tezisda simsiz tarmoqlarga qaratilgan suqilib kirish hujumlarining asosiy turlari, ularda qo‘llaniladigan dasturiy vositalar hamda ularning texnik imkoniyatlari batafsil

tahlil qilindi. Tadqiqotlar shuni ko‘rsatadiki, zamonaviy hujum vositalari ochiq manbalarda keng tarqalgan bo‘lib, ularni ishga tushirish uchun chuqur texnik bilim talab qilinmaydi. Bu esa xavfsizlik tahdidlarining yanada kengayishiga olib keladi. Ayniqsa, Aircrack-ng, Wifiphisher, Hashcat kabi vositalar orqali autentifikatsiyani chetlab o‘tish, foydalanuvchilarni aldash va tarmoq resurslariga zarar yetkazish mumkinligi amaliy misollar bilan asoslab berildi. Shu bilan birga, himoya chorasi sifatida ilg‘or shifrlash algoritmlaridan foydalanish, tarmoq monitoringi, SSID yashirish va WIDS texnologiyalarini joriy etish simsiz tarmoqlar xavfsizligini sezilarli darajada oshirishi mumkin. Tezis natijalari simsiz tarmoqlarni himoya qilish bo‘yicha kompleks yondashuvni shakllantirish va amaliyotga tatbiq etish uchun ilmiy hamda amaliy ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. S.K. Ganiyev, A.A. Ganiyev, Z.T. Xudoyqulov. Kiberxavfsizlik asoslari: o‘quv qo‘llanma. – T.: «Aloqachi», 2020, 303 bet.
2. Maine Basan. Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained, April 29, 2024.
3. Wim Hoogenraad. Black Box Testing: Software, January 23, 2019.
4. Binnie, J. Aircrack-ng Tutorial: Cracking WPA/WPA2 Wi-Fi Passwords. // Ethical Hacking Journal, 2021.
5. Beale J., Kassner L., Bream T., & Liu J. Wireshark & Ethereal Network Protocol Analyzer Toolkit. – Syngress Publishing, 2007. – 528 p.