ISSN 2181-3187

KOMPYUTER TARMOQLARIDA RAZVEDKA HUJUMLARI

Shodimurodov Ulug'bek Akmalovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Nurafshon filiali, talabasi
Jo'rayev Asom Qo'yliboy o'g'li
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Nurafshon filiali, talabasi

ANNOTATSIYA

Ushbu maqolada kompyuter tarmoqlarida razvedka hujumlarining mohiyati, turlari va ularga qarshi kurashish usullari yoritiladi. Razvedka hujumlari axborotni o'g'irlash yoki tarmoq tizimlarining zaifliklarini aniqlash maqsadida amalga oshiriladi. Ushbu maqolada razvedka hujumlarining turli texnikalari, ularning zararli ta'siri va himoya choralariga oid batafsil tahlillar keltirilgan.

Kalit so'zlar: *Kompyuter tarmoqlari, razvedka hujumi, tarmoq xavfsizligi, axborot xavfsizligi, kiberxavfsizlik, himoya choralar*

KIRISH

Kompyuter tarmoqlari bugungi kunda turli tashkilotlar va shaxslar uchun muhim axborot manbai hisoblanadi. Tarmoqlarning keng tarqalishi bilan bir qatorda, ularga nisbatan hujumlar ham ko'paydi. Razvedka hujumlari (yoki skanerlash hujumlari) kiberxavfsizlik sohasida eng ko'p uchraydigan tahdidlardan biridir. Ushbu hujumlar orqali hujumchilar tarmoqda mavjud bo'lgan zaifliklarni aniqlash va keyinchalik ular orqali zararli harakatlar amalga oshirishga urinadilar. Maqolaning maqsadi razvedka hujumlarining mohiyatini, ularning turlarini va ulardan himoyalanish usullarini tahlil qilishdir.

Razvedka hujumlarining mohiyati. Razvedka hujumlari kiberhujumlarning bir turi bo'lib, hujumchilar tarmoq tizimlarining zaifliklarini aniqlashga qaratilgan. Ushbu hujumlar orqali tarmoqdagi kompyuterlar, serverlar va boshqa qurilmalar haqida ma'lumotlar to'planadi. Ma'lumotlar yig'ish jarayonida tarmoq paketlarini skanerlash, portlarni tekshirish, xizmatlarni aniqlash kabi usullar qo'llaniladi.

Hujumlarining turlari. Razvedka hujumlari bir necha turga bo'linadi, jumladan:

Ping skanerlash: Tarmoqdagi qurilmalar mavjudligini aniqlash uchun ping buyrug'idan foydalanish.

Port skanerlash: Qurilmalarda ochiq bo'lgan portlarni aniqlash va ularning qaysi xizmatlarga tegishli ekanligini bilish.

ISSN 2181-3187

Trafik tahlili: Tarmoq orqali o'tayotgan paketlarni kuzatish va tahlil qilish.

Banner grabbing: Tarmoqda ishlayotgan xizmatlarning versiyalari va ularning konfiguratsiyalarini aniqlash.

Razvedka hujumlarining ta'siri. Razvedka hujumlari natijasida hujumchilar tarmoqdagi zaifliklar haqida ma'lumotga ega bo'ladilar. Bu ma'lumotlar keyinchalik yanada xavfli hujumlarni amalga oshirishda qo'llanilishi mumkin. Shu sababli, razvedka hujumlari tarmoqlar xavfsizligi uchun jiddiy tahdid hisoblanadi.

Himoya choralar. Razvedka hujumlariga qarshi samarali himoya qilish uchun quyidagi chora-tadbirlar ko'rilishi mumkin:

Firewall va IDS/IPS tizimlari: Tarmoq trafikini filtrlash va hujumlarni aniqlash tizimlarini qo'llash.

Tarmoqlarni segmentatsiyalash: Tarmoqni kichik segmentlarga bo'lish orqali hujumchilarning kirish imkoniyatlarini cheklash.

Portlarni yashirish va yopish: Tarmoqlarda ishlatilmayotgan portlarni yopish va maxsus portlarni yashirish.

Doimiy monitor va audit: Tarmoqdagi faoliyatni doimiy kuzatish va tahlil qilish.

Xavfsizlik patchlarini o'z vaqtida o'rnatish: Tizimlarning zaifliklarini bartaraf etish uchun xavfsizlik yangilanishlarini o'z vaqtida o'rnatish.

XULOSA

Razvedka hujumlarining kompyuter tarmoqlari uchun o'rnatilgan xavfsizlikni qo'llashda katta o'rin egallashi mumkin. Ushbu hujumlar tarmoqdagi zaifliklarni aniqlab, hujumchilarga tarmoq tizimlariga kirish imkoniyatini beradi. Ammo, zamonaviy xavfsizlik choralarini amalga oshirish, tarmoq tizimlarini razvedka hujumlariga qarshi himoya qilishda katta muhim ahamiyatga ega. Faqatgina shunday qilib, hujumchilarning razvedka hujumlarini amalga oshirish uchun ishlatishlari mumkin.

Razvedka hujumlariga qarshi samarali kurashish uchun zarur xavfsizlik choralari, masalan, firevol va IDS/IPS tizimlari, tarmoqni segmentatsiyalash, portlarni yashirish va yopish, doimiy monitor va audit tizimlari kabi qo'llanmalardan foydalanish juda muhimdir. Ularning yordamida hujumchilarning tarmoqdagi zaifliklarni aniqlash va tizimlarga kirish uchun ishlatishlari osonroq engel bo'lishi mumkin.

Bundan tashqari, tarmoq administratorlari va xavfsizlik mutaxassislarining kiberxavfsizlikni oshirish uchun xavfsizlik patchlarini o'z vaqtida o'rnatish, faqat shu bilan qolmay, tarmoq faoliyatini doimiy kuzatish va tahlil qilish juda muhimdir. Bu usullar orqali tarmoqdagi hujumlarni oldini olish va kompyuter tarmoqlarining xavfsizligini ta'minlash mumkin.

Xulosa qismida keltirilgan ma'lumotlar razvedka hujumlarining o'ziga xos mohiyatini va ularni qarshi olish uchun zarur amalga oshirilishi kerak bo'lgan

ISSN 2181-3187

himoyalash tadbirlarini aks ettiradi. Maqsad hujumchilarning tarmoq tizimlariga kirish imkoniyatini cheklash va tarmoqni xavfsizligini ta'minlashdir.

ADABIYOTLAR RO'YXATI

1. Stallings, W. (2017). "Network Security Essentials: Applications and Standards". Pearson.

2. Scarfone, K., & Mell, P. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". NIST.

3. Easttom, C. (2016). "Network Defense and Countermeasures: Principles and Practices". Pearson IT Certification.

4. Conklin, W. A., White, G. B., Williams, D., Davis, R., & Cothren, C. (2016). "Principles of Computer Security: CompTIA Security+ and Beyond". McGraw-Hill Education.

5. Tittel, E., & Lindros, G. (2019). "Computer Networking First-Step". Cisco Press.