Korporativ tarmoq himoyalanganligini tahlillashning intellektual tizimi

Sayfullayev Sherzod Baxtiyor o‘g‘li,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Axborot xavfsizligi kafedrasi katta o‘qituvchisi,
Toshkent, O‘zbekiston
E-mail: sherzodsay@gmail.uz

Annotatsiya: Maqolada hozirgi zamon kompyuter tarmoqlarining murakkablashishi natijasida yuzaga kelayotgan xavfsizlik muammolari va ularni hal qilish uchun avtomatlashtirilgan intellektual tizim ishlab chiqish masalalari yoritilgan. Tadqiqot doirasida hujumlarning umumiy grafigini shakllantirish va xavfsizlik ko‘rsatkichlarini baholash modellariga asoslangan yondashuv taklif etilgan.

Kalit so‘zlar: korporativ tarmoq, axborot xavfsizligi, intellektual tizim, hujum grafigi, zaiflik tahlili, xavfsizlik ko‘rsatkichlari, xavfsizlik siyosati, buzg‘unchi modeli, avtomatlashtirilgan tahlil, tizim arxitekturasi

Kirish. Hozirgi vaqtda ishlatiladigan kompyuter tarmoqlari, himoya mexanizmlari va dasturiy ta’minot murakkabligining oshishi kuzatilmoqda, bu esa ulardagi zaifliklar sonining ko‘payishiga olib keladi. Tarmoqdagi mavjud zaifliklar va uning konfiguratsiyasi va qo‘llaniladigan xavfsizlik siyosatidagi kamchiliklarning kombinatsiyasidan foydalangan holda, huquqbuzarlar (tashqi va ichki) maqsadlariga qarab turli xil hujum strategiyalarini amalga oshirishlari mumkin. Ushbu strategiyalar turli xil xavfsizlik tahdidlarini amalga oshirishga qaratilgan bo‘lishi mumkin va turli xil xostlarning murosaga kelish zanjirlarini o‘z ichiga oladi.

Shu sababli, kompyuter tarmog‘i ma’muri yoki uning loyihachisi uchun muhim vazifa dastur uchun rejalashtirilgan yoki allaqachon ishlatilgan tarmoq konfiguratsiyasi parametrlari va himoya mexanizmlari kerakli xavfsizlik darajasini ta’minlaydimi yoki yo‘qligini tekshirishdir. Ushbu muammoni hal qilish uchun xavfsizlikni tahlil qilishning avtomatlashtirilgan intellektual vositalari (tizimlari) xizmat qiladi. Bu tizimlar axborotni himoyalash sohasi mutaxassislarining shakllangan bilimlariga asoslanishi, turli buzg‘unchi modellarini, ko‘p qadamli va taqsimlangan xarakterdagi kompyuter hujumlarini hisobga olishi (uning joylashuvi, ko‘nikma va bilim darajasi, harakatlar strategiyasi), korporativ tarmoqlarni va uning komponentalarini himoyalanganligini ko‘rsatuvchi o‘lchov kompleksini hisobini amalga oshirish, korporativ tarmoq va unda amalga oshirilayotgan xavfsizlik siyosatini hisobga olishi kerak. Xavfsizlikni tahlil qilish natijalari “zaif tomonlarni” bartaraf etish va kompyuter tarmog‘ining xavfsizligini oshirish bo‘yicha asosli tavsiyalar ishlab chiqishni ta’minlashi mumkin.

Adabiyotlar tahlili va metodologiya. Roberto Doriguzzi-Corin “Methods and Techniques for Dynamic Deployability of Software-Defined Security Services” (Dasturiy ta'minot bilan ta'minlangan xavfsizlik xizmatlarini dinamik ravishda joylashtirish usullari) (2020) nomli ishida SDN (Software-Defined Networking) va NFV (Network Function Virtualization) texnologiyalarida xavfsizlik xizmatlarini (“security services”) moslashuvchan va dinamik tarzda joylashtirish usullarini ishlab chiqqan. Maqsad — korxona tarmoqlari yoki operator infratuzilmalari uchun resurslar samaradorligini saqlagan holda, tarmoq tahdidlariga tez javob bera oladigan tizimlar yaratishdan iborat. Muhim jihatlari: DDoS hujumlariga qarshi chora-tadbirlar va xavfsizlik xizmatlarini virtualizatsiyalashtirishga erishilgan.

Talal Alharbi “Security in Software Defined Networks” (Dasturiy ta'minot bilan belgilangan tarmoqlarda xavfsizlik) (2018) mavzusidagi ishida SDN infratuzilmasida xavfsizlik xatarlari va zaifliklarning tahlili; nazorat (control) qatlamidagi, topologiya aniqlash (topology discovery), ARP

Handling va virtualizatsiya qatlamlari kabi komponentlarning himoyasi usullari tavsiya etiladi. Korporativ tarmoqlarda SDN qo‘llanilganda ruxsatsiz dasturiy komponentlar orqali controller’ga kirish tahdidlari va ularni kamaytirish bo‘yicha yechimlar taklif qilingan.

Babek Nabiyev “Methods and algorithms for synthesis of network security intellectual monitoring system” (Tarmoq xavfsizligini intellektual monitoring qilish tizimini sintez qilish usullari va algoritmlari) (2017) mavzusidagi ishida tarmoqlarda xavfsizlik monitoringi uchun intellektual tizimni yaratish jarayonlari tavsiflangan. Real vaqt rejimida xavfsizlik holatini baholash, trafikdagi normal yoki kutilmagan (anomaliy) harakatlarni aniqlash, foydalanuvchi profillarini hosil qilish, zararli trafikni tasniflangan. Foydalanuvchi profilini aniqlash uchun klasterizatsiya (clusterization) usuli; tarmoq trafikini ko‘p klassli model orqali tasniflash amalga oshirilgan. Ushbu ilmiy natijalar AzScienceNet tarmog‘ida real sharoitlarda qo‘llanilgan. Ishlab chiqilgan, hujumlarning umumiy grafigini avtomatik ravishda yaratish va yuqori sifatli xavfsizlik ko‘rsatkichlaridan foydalanishga asoslangan yondashuvni amalga oshiradigan xavfsizlikni tahlil qilishning intellektual tizimini taqdim etadi. Yuqoridagilarni hisobga olib mazkur ish mavzusini dolzarb deb hisoblash mumkin.

Hujum grafigi tarmoq konfiguratsiyasi, amalga oshirilayotgan xavfsizlik siyosati, shuningdek, huquqbuzarning joylashuvi, maqsadlari, bilim darajasi va strategiyalarini hisobga olgan holda mumkin bo‘lgan taqsimlangan hujum senariylarini aks ettiradi. Xavfsizlik ko‘rsatkichlari kompyuter tarmog‘ining xavfsizligini turli darajadagi tafsilotlar bilan va turli jihatlarni hisobga olgan holda baholashga imkon beradi [1]. Tadqiqotda xavfsizlikni tahlil qilishning intellektual tizimi uchun ikkita asosiy modeldan foydalanilgan:

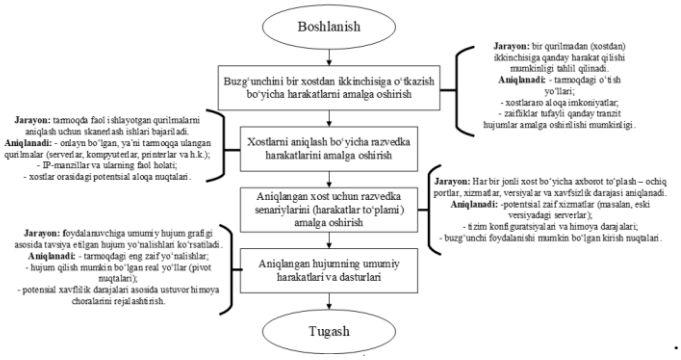
- Hujumlarning umumiy grafigini shakllantirish modeli: ushbu model hujum turlari (razvedka, tayyorgarlik, vakolatlarni egallash va b.) haqidagi ma’lumotlar asosida grafik yaratadi. Kiruvchi ma’lumotlar oldindan beriladi. Grafik ob’ektlari ikki turga bo‘linadi:

1) asosiy ob’ektlar (“Xost” va “hujum harakati”);

2) kompozit ob’ektlar: “marshrut”, “tahdid” va “grafik”.

- Xavfsizlik darajasini baholash modeli: ushbu model xavfsizlik ko‘rsatkichlari (XK) va ularni hisoblash formulalarini o‘z ichiga oladi. Tizimning yakuniy natijasi xavfsizlik darajasini to‘rtta rangli qiymatda (qizil, to‘q qizil, sariq, yashil) taqdim etadi.

Himoyalanganlikni tahlillash intellektual tizimining arxitekturasi. Korporativ tarmoqlari xavfsizligini tahlil qilish uchun ishlab chiqilgan intellektual tizimning arxitekturasi 2-rasmda ko‘rsatilgan. Loyihalash bosqichida himoyalanganlikni tahlillash tizimi (HTT) tahlil qilinadigan tarmoq va xavfsizlik siyosatining berilgan xususiyatlari asosida tahlil qilinadigan kompyuter tarmog‘i (tizimi) modeli bilan ishlaydi [2].



1-rasm. Umumiy hujum grafini shakllantirish algoritmi

Operatsion bosqichda tahlil qilinadigan tarmoq modelini yaratish uchun tahlil qilinadigan kompyuter tarmog‘i haqida ma’lumot to‘plash uchun quyi tizim qo‘llaniladi.

Foydalanuvchi interfeysi moduli foydalanuvchiga tizimning barcha komponentlarining ishlashini boshqarish, kiritilgan ma’lumotlarni o‘rnatish, xavfsizlik tahlili hisobotlarini ko‘rish va h.k. imkonini beradi.

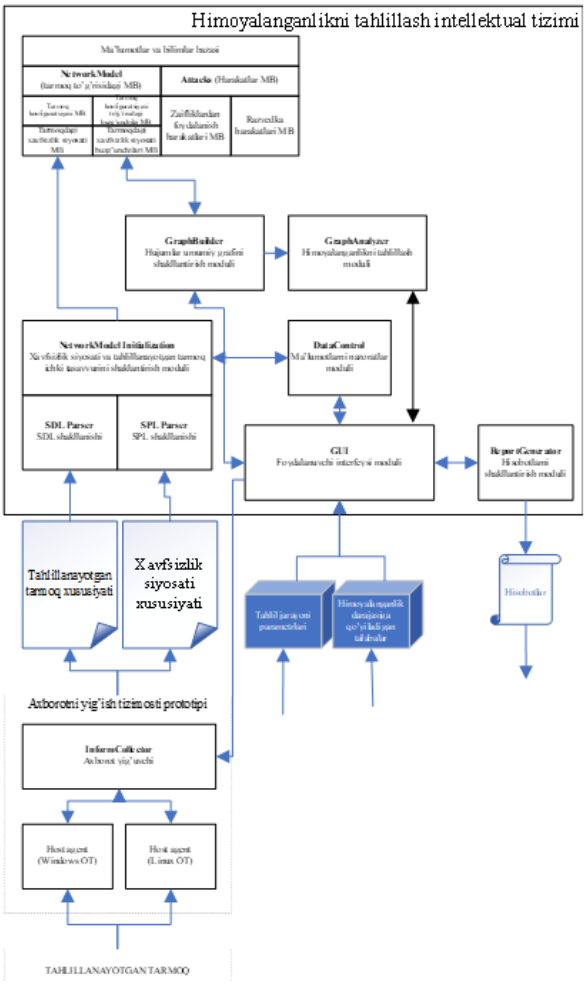
Ma’lumotlar va bilimlar ombori quyidagi ma’lumotlar bazalari guruhlaridan (MB) iborat: (1) tahlil qilinayotgan kompyuter tarmog‘ining konfiguratsiyasi va foydalaniladigan xavfsizlik siyosati (NetworkModel) haqidagi ma’lumotlar bazasi guruhi; (2) hujumkor harakatlar ma’lumotlar bazasi guruhi.

Tahlil qilinayotgan korporativ tarmog‘i haqidagi ma’lumotlar bazalari guruhi quyidagi ma’lumotlar bazalaridan iborat:

- tarmoq konfiguratsiyasi haqidagi ma’lumotlar bazasi;
- tarmoqda amalga oshirilgan xavfsizlik siyosatlarining ma’lumotlar bazasi;
- huquqbuzarning tarmoq konfiguratsiyasi ma’lumotlar bazasi;
- buzg‘unchining tarmoqda amalga oshirilgan xavfsizlik siyosatining ma’lumotlar bazasi.

Tarkibiy jihatdan ma’lumotlar bazasi ma’lumotlari ikki xil (tarmoq konfiguratsiyasi bo‘yicha ma’lumotlar bazalari va unda amalga oshirilgan xavfsizlik siyosati mos ravishda) bo‘lib, tarmoq arxitekturasi (masalan, ishlatiladigan operatsion tizimlarning turlari va versiyalari, ilovalar, ochiq portlar ro‘yxati va boshqalar) hamda tarmoqning ishlashini tavsiflovchi qoidalar to‘g‘risidagi ma’lumotlarni o‘z ichiga oladi [3-4].

Hujum harakatlarining ma’lumotlar bazasi guruhi quyidagi ma’lumotlar bazalaridan iborat: (1) zaifliklardan foydalanish harakatlarining ma’lumotlar bazasi; razvedka operatsiyalari ma’lumotlar bazasi. Zaifliklardan foydalanadigan harakatlar ma’lumotlar bazasi (ushbu guruhdagi boshqa ma’lumotlar bazalaridan farqli o‘laroq) zaifliklarning tashqi ma’lumotlar bazasi asosida qurilgan.



2-rasm. Himoyalanganlikni tahlillash intellektual tizimining arxitekturasi

Ushbu ma’lumotlar bazasidagi hujum harakatlari quyidagi guruhlarga bo‘linadi:

1) mahalliy foydalanuvchi huquqlarini olishga qaratilgan harakatlar;

2) administrator huquqlarini olishga qaratilgan harakatlar;

3) maxfiylik;

4) butunlilik

5) foydalanuvchanlikni buzishga qaratilgan harakatlar.

Intelligence Activity DB host yoki tarmoq haqida masofadan turib ma’lumot olishga qaratilgan faoliyatni o‘z ichiga oladi. Razvedka faoliyati tavsiflari tashqi zaiflik ma’lumotlar bazalarida mavjud emas. Huquqbuzar tomonidan razvedka faoliyatini amalga oshirish usullari va vositalari to‘g‘risidagi ma’lumotni faqat ekspertiza vositalari orqali olish mumkin.

NetworkModel Initialization foydalanuvchi tomonidan ko‘rsatilgan tarmoq konfiguratsiyasi va unda amalga oshirilgan xavfsizlik siyosati haqidagi ma’lumotlarni (bu ma’lumotlar tizim System Description Language (SDL) va Security Policy Language (SPL) ixtisoslashtirilgan tillar yordamida belgilanadi) ichki ko‘rinishga aylantiradi.

DataControl xavfsizlikni tahlil qilish jarayoni uchun zarur bo‘lgan noto‘g‘ri ko‘rsatilgan yoki etishmayotgan ma’lumotlarni aniqlash uchun ishlatiladi. Masalan, foydalanuvchi noto‘g‘ri xizmat nomini kiritishi yoki 21-port ochiqligini ko‘rsatishi mumkin, lekin qaysi ilova ushbu portga kelgan so‘rovlarni ko‘rib chiqayotganini aniqlay olmaydi.

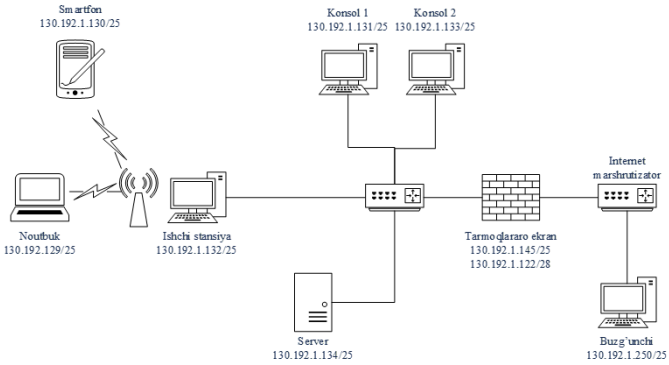
GraphBuilder tahlil qilinayotgan kompyuter tarmog‘idagi tajovuzkorning harakatlarini taqlid qilish va mavjud bo‘lgan har xil turdagi hujum harakatlari (zaifliklardan foydalanadigan hujum harakatlari, razvedka harakatlari, qonuniy foydalanuvchilarning oddiy harakatlari), tarmoq konfiguratsiyasi va unda amalga oshirilgan xavfsizlik siyosati haqidagi ma’lumotlardan foydalangan holda umumiy hujum grafigini yaratadi. Ushbu modul asosiy ob’ektlarning xavfsizlik ko‘rsatkichlarini grafik cho‘qqilariga joylashtiradi, buning asosida GraphAnalyzer kompozit ob’ektlar ko‘rsatkichlarini hisoblab chiqadi.

ReportGenerator xavfsizlik tahlili davomida olingan ma’lumotlarni (aniqlangan zaifliklar to‘g‘risidagi ma’lumotlar, xavfsizlik darajasini oshirish bo‘yicha tavsiyalar) jamlash va ular asosida yagona hisobot yaratish uchun ishlatiladi [5-6].

Axborot yig‘ish quyi tizimi dasturiy ta’minot xost agentlaridan ma’lumotlarni yig‘ish va shu ma’lumotlarga asoslanib, tarmoq konfiguratsiyasi va unda amalga oshirilgan xavfsizlik siyosatini tavsiflovchi spetsifikatsiyalarni yaratish uchun ishlatiladi. Xost dasturiy ta’minot agentlari tahlil qilinayotgan kompyuter tarmog‘ining modelini yaratish uchun zarur bo‘lgan ma’lumotlarni to‘plash uchun ishlatiladi. Masalan, ushbu agentlar operatsion tizimning konfiguratsiya fayllari va turli xil dasturiy vositalar tahlilini amalga oshirishi mumkin. InformCollector xost agentlaridan keladigan ma’lumotlarni yig‘ish, uni SDL va SPLda taqdim etish va SAZ (NetworkModel Initialization moduli) komponentlariga o‘tkazish uchun ishlatiladi [7-8].

Natijalar. Quyida sinov korporativ tarmoq ko’rib chiqiladi (3-rasm). Umumiy hujum grafini qurish jarayonida hujum qiluvchining hujum qilingan tarmoqni tushunishida quyidagi asosiy o‘zgarishlar sodir bo‘ladi (4-rasm):

- “ping” hujumini amalga oshirgandan so‘ng (trafik marshrutlash jadvalini hisobga olgan holda) buzg‘unchi “Server” xostining mavjudligi haqida bilib oladi (4,a-rasm);
- buzg‘unchi FTP xizmatidagi zaiflikdan foydalanadigan va masofaviy buzg‘unchiga mahalliy ma’mur huquqlarini qo‘lga kiritish imkonini beruvchi hujumni amalga oshiradi (“Server” xosti qizil rang bilan belgilangan) (4,b-rasm);



3-rasm. Sinov korporativ tarmog‘ining tuzilishi

- buzg‘unchi barcha mavjud ma’lumotlarni to‘plash uchun “Server” xostiga ega bo‘lgan huquqlardan foydalanadi, tahlil qilish orqali buzg‘unchi portni yo‘naltirish qo‘llanilishini va “Server” xosti boshqa tarmoq markaziga ulanganligini tushunadi. Shuning uchun, buzg‘unchi uchun “Server” xostiga o‘tish foydalidir, chunki bunday o‘tish buzg‘unchi uchun boshqa tarmoq segmentiga kirishni ochadi (4,d-rasm);
- “Server”ga o‘tish orqali buzg‘unchi “ping” hujumini amalga oshiradi va u ketma-ket hujum qilishga harakat qiladigan boshqa ko‘plab xostlar mavjudligini bilib oladi (4,e-rasm).

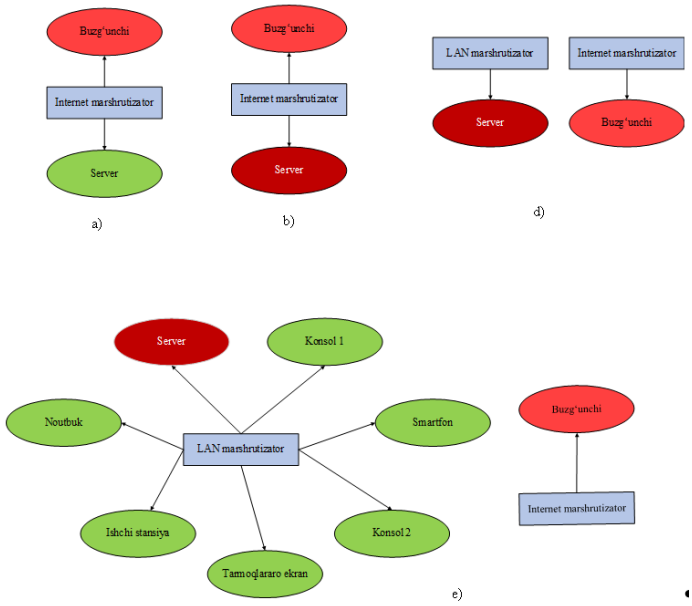
Xavfsizlikni tahlil qilish jarayonining asosiy natijalari:

- aniqlangan zaifliklar to‘plami;

- xavfsizlik ko‘rsatkichlari to‘plami (masalan, “Server” xosti orqali o‘tadigan hujum yo‘llari soni).

Sinov kompyuter tarmog‘i uchun xavfsizlik tahlili natijasida “qizil” xavfsizlik darajasi olindi. Foydalanuvchining keyingi qadamlari quyidagilardan iborat bo‘lishi kerak:

1) aniqlangan zaifliklar va to‘siqlarni bartaraf etish (tarmoq konfiguratsiyasini va amalga oshirilgan xavfsizlik siyosatini yangilash);
2) yangilangan xususiyatlar bilan aniqlangan tarmoq xavfsizligini qayta tahlil qilish.



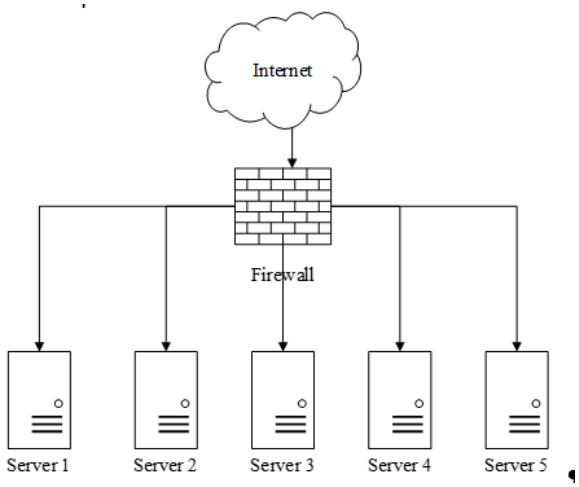
4-rasm. Buzg‘unchining hujum qilingan korporativ tarmog‘i haqidagi tasavvurini o‘zgartirish

Korporativ tarmoq xavfsizligini oshirish usulini qo‘llash samaradorligini baholash. Xavfsizlik nuqtai nazaridan usulni qo‘llash samaradorligi tushunchasi shuni anglatadiki, tarmoq xavfsizligining umumiy darajasining oshishi (yaxshilanishi) yoki pasayishi (yomonlashishi) miqdorini aniqlash kerak. Korporativ tarmoq xavfsizligini uning tuzilishi bo‘yicha oshirish usuli tarmoqqa kirishni cheklash vositalaridan foydalangan holda xavfsizlik domenlarini ajratish va keyinchalik birlashtirishdan iborat. Xavfsizlik domenlarini tanlash amaliyotidan oldin, dastlabki ma’lumotlarga asoslanib, tarmoq hozirgi holatida domenlarga qanday bo‘linishini aniqlash kerak. Keyin, domenlarni ajratgandan so‘ng, olingan natijani dastlabki domen bo‘linishi bilan solishtirish lozim.

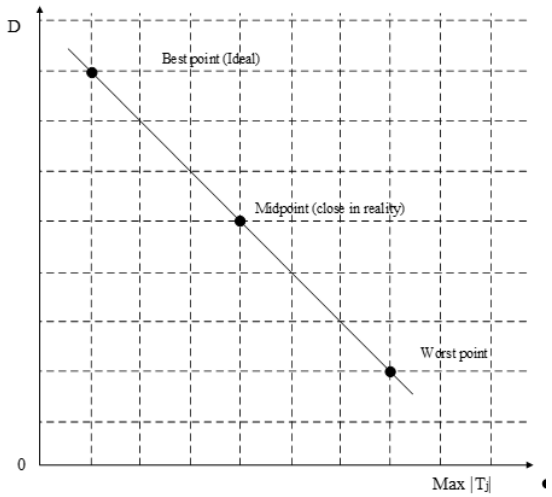
Jotiy tarmoq domenlari miqdorini D_{bosh} va joriy tarmoq ahr bir xavfsizlik domeni xususiyatlari vektorini $\overline{T_{bosh}}$ deb belgiladi. D_{bosh} va $\overline{T_{bosh}}$ mos holda domenlar miqdori va tarmoq har bir domeni xususiyatlari (servislari) vektori bo‘ladi.

Agar $\|\overline{T_{bosh}}\|$ boshlang‘ich tarmoq barcha vektorlari xususiyatlari miqdori deb va $\|\overline{T_{yak}}\|$ natijaviy tarmoq barcha vektorlari barcha xususiyatlari miqdori deb hamda $|\overline{T_{bosh}}|$ boshlang‘ich tarmoq vektorlari miqdori deb va $|\overline{T_{yak}}|$ natijaviy tarmoq vektorlari miqdori deb qabul qilinsa, unda

$$\left|\|\overline{T_{bosh}}\|\right| = \left|\|\overline{T_{yak}}\|\right|, biroq\ |\overline{T_{bosh}}| \neq |\overline{T_{yak}}|.$$



5-rasm. Samaradorlikni baholashda korporativ tarmoqqa misol



6-rasm. Domenlar miqdorini domenlardagi obyektlarning maksimal miqdoriga nisbatining xavfsizlik darajasiga bog‘liqligi grafigi

Bunda quyidagi tengsizlik bajarilishi lozim:

$D_{bosh} \leq D_{yak}$.

Tarmoq xavfsizligining ikkita cheklangan variantini ko‘rib chiqiladi: mutlaqo xavfsiz va mutlaqo himoyalanmagan tarmoq.

Birinchi variantda har bir vektor o‘lchami $\left|\overline{T_{yak_j}}\right| = 1, \forall j \in [1, D_{yak}]$. Ya’ni, har bir xavfsizlik domenida faqatgina bitta servis mavjud.

Ikkinchi variantda $D_{yak} = 1$, ya’ni barcha servislar bitta domenda joylashgan.

Bu ikki variant orasidagi boshqa har qanday hol quyidagi shartlarda nisbatan xavfsiz (ideal holat deb qaralsa) deb hisoblanadi:

$D_{bosh} \to max$ va $\left|\overline{T_{yak_j}}\right| \to 1$, bir vaqtda.

Bundan ko‘rinib turibdiki, $\max(D_{bosh}) = \left|\left|\overline{T_{yak}}\right|\right|$.

Bu shuni anglatadiki, tarmoqni iloji boricha kamroq xizmatlar bilan ko‘proq xavfsizlik domenlariga bo‘lish ushbu tarmoq xavfsizligining umumiy darajasini oshirish uchun zaruriy shartdir.

Grafikda (6-rasmda) yuqorida aytilganlarning barchasini ko‘rish mumkin. Xavfsizlik nuqtai nazaridan eng yuqori nuqta ideal, eng past nuqta esa eng yomon nuqta hisoblanadi. Ox o‘qi bo‘yicha $\max |\overline{T_j}|$ (vektorlar xususiytalari har bir xususiyatlari miqdorini maksimumi), Oy o‘qi bo‘yicha D qo‘yilgan.

Xulosa. Xulosa o‘rnida shuni ta’kidlash mumkin-ki, zaiflik tahlilini amalga oshirish va kompyuter tarmoqlarining hayot siklning turli bosqichlarida xavfsizlik darajasini baholash uchun mo‘ljallangan himoyalaganlikni tahlillash intellektual tizimi ko‘rib chiqildi. Taklif etilayotgan intellektual xavfsizlik tizimining ishlashi quyidagi xususiyatlarga ega bo‘lgan yondashuvga asoslanadi:

- xavfsizlikni tahlil qilish uchun ekspert bilimlari asosida qurilgan turli modellar to‘plamidan foydalanish, shu jumladan buzg‘unchi modellari, hujum senariysi modellari, hujumlar grafini shakllantirish, xavfsizlik ko‘rsatkichlarini hisoblash va xavfsizlikning umumiy darajasini aniqlash;
- buzg‘unchining joylashuvi, maqsadlari va bilim darajasining xilma-xilligini hisobga olgan holda;
- umumiy hujum grafni tuzishda nafaqat kompyuter tarmog‘i konfiguratsiya parametrlaridan, balki amalga oshirilgan xavfsizlik siyosati qoidalaridan ham foydalanish;
- haqiqiy hujum harakatlarini (zaifliklardan foydalangan holda) va ruxsat etilgan foydalanuvchi harakatlari va razvedka harakatlarini hisobga olish;
- turli xil tarmoq resurslariga turli xil xavfsizlik tahdidlarini o‘rganish qobiliyati;
- “to‘siqlarni” aniqlash qobiliyati (eng ko‘p hujum yo‘llari va murosaga kelish uchun eng yuqori potentsialga ega bo‘lgan zaifliklar uchun mas’ul bo‘lgan xostlar);
- tizimga “agar” ko‘rinishidagi so‘rovlarini berish imkoniyati, masalan, tarmoq konfiguratsiyasining ma’lum parametri yoki xavfsizlik siyosati qoidasi o‘zgartirilganda xavfsizlik qanday bo‘ladi;
- hujum grafini yaratish uchun yangilangan zaiflik ma’lumotlar bazalaridan foydalanish;
- asosiy xavfsizlik ko‘rsatkichlarining bir qismini hisoblash uchun CVSS yondashuvidan foydalanish;
- xavfsizlik ko‘rsatkichlarini hisoblash uchun xavflarni sifatli tahlil qilish usullaridan (xususan, o‘zgartirilgan SANS/GIAC tarmoq hujumining jiddiyligini baholash usuli va FRAP usuli) foydalanish.

Foydalanilgan adabiyotlar

1. Stallings, William & Brown, Lawrie. (2018). Computer security: principles and practice / William Stallings, Lawrie Brown, UNSW Canberra at the Australian Defence Force Academy. Hoboken, New Jersey: Pearson Education, Inc. https://nla.gov.au/nla.cat-vn7464940
2. Kott, A., Wang, C., & Erbacher, R. F. (2015). Cyber defense and situational awareness (Vol.

62). Springer. https://doi.org/10.1007/978-3-319-11391-3 .

3. Bal, J. (2020). A review of attack graph and attack tree visual syntax in cyber security. Computer Science Review. https://www.academia.edu/105575918/A_review_of_attack_graph_and_attack_tree_visual_syntax_in_cyber_security

4. Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN COMPUT. SCI.* **2**, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0 .

5. FIRST. (2025). "Common Vulnerability Scoring System (CVSS) v4.0: User Guide." https://web.archive.org/web/20250125085936/https://www.first.org/cvss/v4-0/ .

6. SANS Institute. (2024). "Network Attack Severity Assessment and Risk Analysis Framework." *SANS Reading Room.* https://www.prweb.com/releases/sans-institute-unveils-highly-anticipated-annual-security-awareness-report-for-2024-302209886.html

7. Fu, C., Zhang, H. & Zhou, Y. An approach to generating attack graphs and analyzing threats based on CAPEC and ATT&CK matrix. *Softw Syst Model* (2025). https://doi.org/10.1007/s10270-025-01328-8

8. Chauhan, Jaskirat. (2025). Automated Security Configuration Management for Enterprise Networking Products. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 11. 2881-2888. DOI: 10.32628/CSEIT251112296.