№ 2/1(40) 2022

ISSN 2181-8460

HISOBLASH VA AMALIY MATEMATIKA MUAMMOLARI

ПРОБЛЕМЫ ВЫЧИСЛИТЕЛЬНОЙ И ПРИКЛАДНОЙ МАТЕМАТИКИ

PROBLEMS OF COMPUTATIONAL AND APPLIED MATHEMATICS

RAQAMLI TEXNOLOGIYALAR VA
SUN'IY INTELLEKTNI RIVOJLANTIRISH
ILMIY-TADQIQOT INSTITUTI

ПРОБЛЕМЫ ВЫЧИСЛИТЕЛЬНОЙ И ПРИКЛАДНОЙ МАТЕМАТИКИ

Спецвыпуск № 2/1(40) 2022

Журнал основан в 2015 году.
Издается 6 раз в год.

Учредитель:
Научно-исследовательский институт развития цифровых технологий и искусственного интеллекта.

Журнал зарегистрирован в Агентстве информации и массовых коммуникаций при Администрации Президента Республики Узбекистан.
Регистрационное свидетельство №0856 от 5 августа 2015 года.

ISSN 2181-8460, eISSN 2181-046X

Адрес редакции:
100125, г. Ташкент, м-в. Буз-2, 17А.
Тел.: +(99871) 231-92-45.
E-mail: info@pvpm.uz.
Сайт: www.pvpm.uz.

Дизайн и компьютерная вёрстка:
Шарипов Х.Д.

Отпечатано в типографии НИИ РЦТИИ.
Подписано в печать 29.04.2022 г.
Формат 60x84 1/8. Заказ №2. Тираж 100 экз.

Содержание

УУК 004.95

ТАРМОҚ ТРАФИГИНИ ТАҲЛИЛ ҚИЛИШ ТИЗИМИНИ ИШЛАБ ЧИҚИШ

[1]Абдуллаева Б.М., [2]Самижонов Б.Н., [3]Ережепов К.К., [1]Жўраева М.А., [1]Абдувахобов Ф.Ф.

[1] Наманган давлат университети,
160107, Ўзбекистон, Наманган, Бобуршох, 161;
[2] Тошкент шаҳридаги Инха университети,
100170, Ўзбекистон, Тошкент, Зиёлилар, 9;
[3] Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Нукус филиали,
230101, Ўзбекистон, Нукус, А.Досназаров, 74.

Ушбу мақолада рухсат ўтилмаган фаолликни таҳлил қилиш ва аниқлаш учун тармоқ трафигини йиғиш учун прототип тизимини ишлаб чиқиш ҳамда тизимнинг зарур функционаллиги локал тармоқдан ташқи Интернетга чиқадиган тармоқ трафигини қабул қилиш, сақлаш, қайта ишлаш ва визуаллаштириш масаласи кўриб чиқилган.

Иш жараёнида тармоқ трафигини таҳлил қилишнинг замонавий усуллари ўрганилди, тизим архитектураси ишлаб чиқилди, статистик трафикни қайта ишлаш алгоритмлари яратилди ва тармоқдан олинган реал маълумотларда тизимнинг ишлаши синовдан ўтказилди. Тизим прототипи чиқиш маршрутизатори яқинидаги тармоқ инфратузилмасига уланиб, унинг статистикасини қулай шаклда тақдим этиш учун трафик тўпламини қайта ишлаш имконини беради.

Калит сўзлар: тармоқ, трафик, тизим, маълумот, прототип, визуал, ҳужум.

Иқтибос: *Абдуллаева Б.М., Самижонов Б.Н., Ережепов К.К., Жўраева М.А., Абдувахобов Ф.Ф.* Тармоқ трафигини таҳлил қилиш тизимини ишлаб чиқиш // Проблемы вычислительной и прикладной математики. – 2022. – № 2/1(40). – С. 19-30.

1 Кириш

Тармоқларни тез оммалашиши ва ривожланиши ҳисоблаш тизимларини сезиларли даражада мураккаблаштирди. Уларни бир-бирига нисбатан боғлиқ бўлиши зарарли ҳаракатлардан камроқ ҳимояланганлик ҳолатини келтириб чиқарди. Ахборотни қайта ишлаш, сақлаш ва узатишни автоматлаштириш даражасининг ўсиши хавфсизлик муаммоларининг пайдо бўлишига ҳам таъсир қилади ва бузғунлар натижасида юзага келадиган йўқотишларни қоплаш харажатлари доимий равишда ошиб бормоқда [1].

Компютер тизимлари ва тармоқларига ҳужумлар сонини кўпайишининг барқарор тенденцияси мавжуд [2]: масофавий таъсир қилиш усуллари ва ёндашувлари доимий такомиллаштирилмоқда. Шунинг учун мавжуд ҳимоя тизимлари бундай ўзгаришларга ўз вақтида жавоб беришга имкон бермайди. Чунки аввал тармоқ ҳужумини аниқлаш, кейин эса ўрганиш керак. Зарарли трафикни бутунлай чиқариб юборишни ҳозирги кунда ҳеч қандай усули мавжуд эмас. Ушбу ҳолатлар рухсат этилмаган трафикни аниқлашнинг самарали усуллари ва ахборотни ҳимоя қилиш воситаларини ишлаб чиқиш долзарб эканлигини билдиради.

Ҳозирги кунда ҳужумларни аниқлаш ва олдини олишнинг турли усуллари фаол ишлаб

чиқилмоқда ва қўлланилмоқда, бироқ улар амалда ҳар доим ҳам самарали натижаларни таъминламаяпти. Бу эса барча ҳимоя технологиялари доимий равишда ўрганишни ва такомиллаштиришни талаб қилади.

Мавжуд тизимларни умумий хусусияти бу локал тармоқни ташқи томондан зарарли таъсирлардан ҳимоя қилиш учун бирлаштириши ҳисобланади. Администратор ўз вақтида чоралар кўришга тезкор қарор қилиши ва шу билан ташқи тармоқни локал тармоқ таъсиридан ҳимоя қилиши мумкин. Агар бундай схема кўпгина кичик тармоқларнинг ишлашига кенгайтирилса, у ҳолда тармоқ инфратузилмаси хавфсизлиги янги даражага кўтарилади. Шунинг учун ушбу ишда рухсат этилмаган фаолликнини таҳлил қилиш ва аниқлаш учун тармоқ трафигини йиғиш учун прототип тизимини ишлаб чиқиш масаласи қаралган. Мақсадга эришиш учун қуйидаги вазифаларни ҳал этиш талаб қилинади:

тармоқ хавфсизлиги муаммосини ва тармоқ трафигини таҳлил қилишнинг замонавий усул ва воситаларини ўрганиш;

оптимал тизим архитектурасини ишлаб чиқиш;

олинган маълумотларни статистик қайта ишлаш алгоритмларини яратиш;

ишлаб чиқилган архитектура ва алгоритмлар асосида зарарли трафикни аниқлаш учун дастурий таъминот тизимининг прототипини жорий этиш.

Ахборотни қайта ишлаш ва сақлаш жараёнида ушбу жараён иштирокчилари ўртасида маълумотлар алмашинуви зарурати юзага келади. Айни пайтда локал ва глобал тармоқлар ривожланишда давом этмоқда, маълумотларни узатишнинг янги протоколлари пайдо бўлмоқда, тармоқ ускуналари аппарат имкониятлари кенгаймоқда, уланган абонентлар сони ва умумий трафик ҳажми ошиб бормоқда. Соҳанинг бундай жадал ривожланиши қатор муаммоларни келтириб чиқармоқда. Улардан бири ахборот хизматлари истеъмолчилари сони ортиб бориши билан хизмат кўрсатиш сифати даражасини сақлаб қолиш учун фойдаланиладиган тармоқ ва сервер ускуналарига қўйиладиган талаблардир. Иккинчиси тармоқ ичида айланувчи ахборотни ҳимоя қилиш зарурлигига асосланади [3].

Ушбу муаммоларни ҳал қилиш учун тармоқ ускуналарини узоқ вақт давомида ишламай қолишига йўл қўймайдиган, муаммоларни самарали ташхислаш ва ҳал қилишга ёрдам берадиган трафик мониторинги ва таҳлилидан фойдаланилади [4]. Маълумотлар тармоқ орқали деярли узлуксиз узатилганлиги сабабли, ускунанинг ишлашини тўхтатиш ёки хизмат кўрсатишни рад этишнинг бошқа сабаблари хизматлар кўрсатувчи ташкилотлар ёки компаниялар учун йўқотишларга олиб келиши аниқ. Натижада, администраторлар тармоқ трафиги ҳаракати ва бутун тармоқнинг ишлашини кузатиши, шунингдек, хавфсизлик сиёсатидаги бўшлиқларни доимий текширишлари керак.

Мониторинг ва таҳлилни таклиф қилувчи воситалар. [5] иш муаллифлари компютер тармоқларини қуйидаги гуруҳларга ажратишган:

Тармоқларни бошқариш тизимлари (Network Management Systems) - тармоқ қурилмалари ҳолати тўғрисидаги маълумотлар ва тармоқ трафиги ҳақида маълумотларни йиғувчи марказлаштирилган дастурий таъминот тизимлари. Ушбу дастурларнинг функционаллиги тармоқ мониторинги ва таҳлили билан чекланмайди. Улар автоматик ёки ярим автоматик режимда тармоқни бошқаришни амалга оширади, яъни калитлар ва бошқа жиҳозларнинг манзил жадвалларини ўрнатиш ва ўзгартириш, қурилма портларини ёқиш ёки ўчириш. Бундай тизимларга HPOpenView, SunNetManager, IBMNetView каби тизимлар мисол бўлади.

Ўрнатилган диагностика ва назорат тизимлари (Embedded systems). Ушбу турдаги тизимлар алоқа ускуналарига ўрнатиладиган дастурий таъминот ва аппарат модуллари шаклида ёки операцион тизимда дастурий модуллар шаклида амалга оширилади. Улар фақат улар жойлашган қурилмани бошқариш ва ташхислаш имконини беради. Бундай тизимларга мисол сифатида Distributed 5000 концентратор бошқарув модули мисол бўла олади, у носозликларни аниқлагандан сўнг портларни авто-сегментлаш, марказ ички сегментларига портларни белгилаш ва бошқалар функцияларини бажаради. Одатда, ўрнатилган бошқарув модуллари SNMP агентлари сифатида ҳам ишлайди, бошқарув тизимига қурилма ҳолати ҳақида хабар беради.

Тизим бошқарув воситалари (System Management). Ушбу гуруҳнинг ускуналари бошқа объектларга нисбатан бошқарув тизимларига ўхшаш функцияларни бажаради. Бошқарув объекти тармоқ компютерлари дастурий ва техник воситалари ҳамда алоқа ускуналари ҳисобланади.

Протокол анализаторлари (Protocol analyzers) - бу фақат тармоқлардаги трафикни кузатиш ва таҳлил қилиш учун фойдаланиладиган дастурий ёки аппарат-дастурий тизимлар. Яхши анализатор - бу тармоқларда қўлланиладиган кўп сонли протоколлар пакетларини ушлай оладиган ва декодлай оладиганлари ҳисобланади. Ушбу тизимлар гуруҳи алоҳида пакетларни ушлаши учун баъзи мантиқий шартларни ўрнатиши ва пакетларни тўлиқ декодланишини амалга ошириши мумкин, яъни ҳар бир пакет майдонининг мазмунини декодлаш билан фойдаланувчи учун қулай шаклда турли даражадаги протокол пакетларини жойлаштиришни кўрсатиш.

Тармоқни лойиҳалаш ёки янгилаш бошлаганда кўпинча тармоқ хусусиятларини миқдорий баҳолашга эҳтиёж туғилади. Масалан, турли босқичларда юзага келадиган кечикишлар, селектив ҳодисаларни пайдо бўлиш частотаси, алоқа линиялари бўйлаб маълумотлар оқими интенсивлиги, сўровларга жавоб бериш вақтлари ва бошқалар.

Кабел тизимларини ташхислаш ва сертификатлаш ускуналари. Ушбу гуруҳнинг мақсади номидан аниқ, анъанавий бундай ускуналарни тўртта кичик гуруҳга ажратиш мумкин: кабел сканерлари, тармоқ мониторлари, мултиметрлар ва кабел тизимларини сертификатлаш қурилмалари.

Эксперт тизимлари инсоннинг тармоқларни аномал ишлаши сабабларини аниқлаш ва тармоқни иш ҳолатига қайтариш мумкин бўлган усулларини бирлаштиради. Кўпинча улар юқорида муҳокама қилинган бошқа тармоқ мониторинги ва таҳлил воситаларини алоҳида қуйи тизимлари сифатида тақдим этилади.

Эксперт тизимининг оддий версияси контекстга сезгир ёрдам тизимини ўз ичига олади, мураккаброқлари эса сунъий интеллект элементларига эга бўлган билим базалари деб аталади. Ушбу гуруҳга мисол сифатида Cabletron нинг Spectrum бошқарув тизимига ўрнатилган қўшимча тизимни келтириш мумкин.

Таҳлил ва ташхис учун кўп функцияли қурилмалар. Локал тармоқларнинг кенг қўлланилиши бир нечта қурилмаларни функционаллиги асосида арзон портатив қурилмаларни ишлаб чиқишни талаб қилади: кабел сканерлари, тармоқни бошқариш дастурлари ва протокол анализаторлари. Масалан, MicrotestInc компаниясининг Compas ёки FlukeCorp компаниясининг 675 LANMeter тизимлари. Бундан ташқари, тармоқни кузатишнинг яна иккита усулини, яъни ва йўналтирилмаган. Маршрутизаторга йўналтирилган усулда йўриқнома тўғридан-тўғри ичига ўрнатилган мониторинг ва бошқа дастурларни қўшимча ўрнатишни талаб қилмайди. Иккинчи усул, мос равишда, маршрутизаторларга қаратилмайди, яъни бу мутахассиснинг ўзи томонидан жорий эҳтиёжлар учун танланган зарур аппарат ва дастурий таъминотдир.

Ҳужумларни аниқлаш ва олдини олиш тизимлари. Ахборотни ҳимоя қилиш учун бундай тизимларни жорий этиш жиддий тармоқ инфратузилмаларини барчаси учун зарур ҳисобланади, чунки глобал тармоққа уланган ҳар қандай ускунада доим заифликларни излайдиган дастурлар мавжуд. Масалан, Shodan қидируви [6] автоматик равишда хавфсизлик тизимининг бирон бир қисмига эга бўлмаган уланган қурилмалар ҳақида маълумот тўплайди. Бузилишларни аниқлаш ва олдини олиш тизимлари бундай таъсирга қарши қаратилган, шунинг учун улар хавфсизлик сиёсатида тез-тез фойдаланиладиган воситадир [7].

Ҳужумларни аниқлаш тизими (ҲАТ) (инг. Intrusion Detection System (IDS))— компютер тизими ёки тармоғига рухсат этилмаган киришни аниқлашга мўлжалланган дастурий ёки аппарат воситаси.

Ҳужумларни олдини олиш тизими (ҲООТ) (инг. Intrusion Prevention System (IPS))) бу зарарли фаолиятни аниқлаш, олдини олиш ёки блокировка қилиш мақсадида реал вақтда тармоқ ёки тизимни кузатувчи дастурий ёки аппарат воситасидир.

Ҳужумнинг олдини олиш тизимлари ҳужумларни аниқлаш тизимларининг кенгайтмаси деб ҳисобланиши мумкин, чунки бунда ҳужумларни кузатиш вазифаси бир хил бўлиб қолади.

Аммо ҲООТ ҳужумларни реал вақтда кузатиши ва ҳужумларни олдини олиш учун дарҳол ҳаракат қилиши керак. Бунинг учун улар қуйидагилардан фойдаланадилар: уланишларни қайта ўрнатиш, тармоқдаги трафик оқимларини блокировка қилиш, операторга сигналларни бериш. Бундан ташқари, бундай тизимлар пакетларни дефрагментациялаши, SEQ ва АСК ўзгарган пакетлардан ҳимоя қилиш учун TCP пакетлар тартибини ўзгартириши мумкин [8].

Ушбу тизимлар компютер тизими ёки тармоғида содир бўладиган ҳодисаларни кузатиш ва хавфсизлик муаммолари белгиларини излаш учун ҳодисаларни таҳлил қилиш жараёнини автоматлаштиришда қўлланилади. Сўнгги пайтларда тармоққа рухсат этилмаган тажовузларни ташкил этишнинг турли усуллари ва турлари сони сезиларли даражада ошганлиги сабабли, ҳужумларни аниқлаш тизимлари кўпчилик ташкилотлар учун хавфсизлик инфратузилмасининг ажралмас қисмига айланди. Бунга потенциал тажовузкорлар синчковлик билан ўрганадиган ушбу масала бўйича катта ҳажмдаги адабиётлар ва ахборот тизимларига киришга уринишларни аниқлашнинг тобора мураккаб ёндашувлари ёрдам беради.

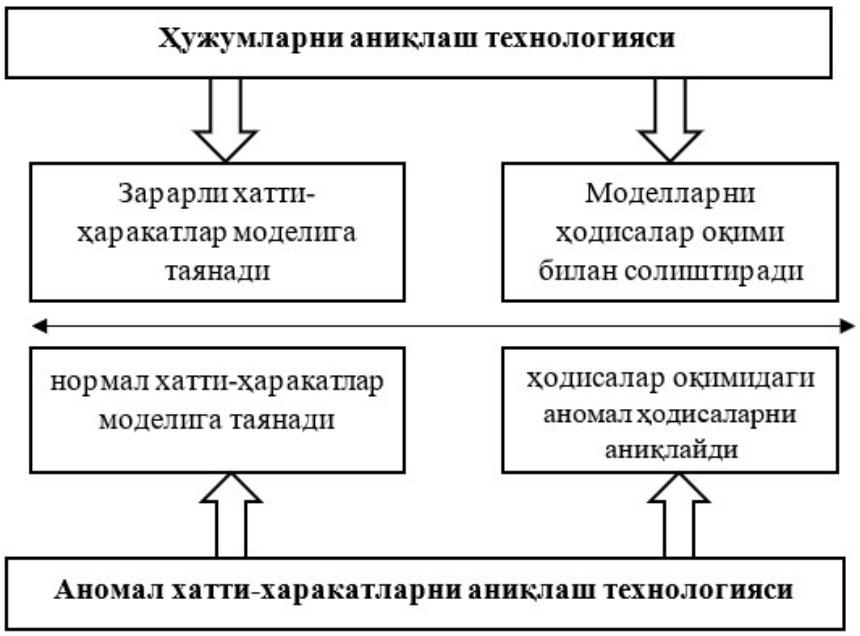
Ҳужумларни аниқлашнинг замонавий тизимлари турли хил архитектурага эга, уларнинг асосийлари тармоқ ва локалдир. Тармоқ тизимлари локал тармоқ орқали ўтадиган трафикни таҳлил қилиш учун махсус компютерларга ўрнатилади. Одатда локал тизимлар ҳимояга муҳтож бўлган ва муайян ҳодисаларни ўрганадиган компютерларда жойлашган бўлади.

ҲАТ архитектурасидан ташқари, уларни аниқлаш усули билан ҳам ажратиш мумкин: баъзи тизимлар аномал ҳатти-ҳаракатни, иккинчиси -зарарлиларни қидиради [9].

Аномал ҳатти-ҳаракатларини аниқлаш тизимлари (инглизча anomaly detection) ҲАТ кузатиш объектининг тўғри ёки мақбул ҳатти-ҳаракатларини тавсифловчи белгиларни билишига асосланади. "Оддий" ёки "тўғри" ҳатти-ҳаракатлар деганда объект томонидан хавфсизлик сиёсатига зид бўлмаган ҳаракатлар тушунилади [8].

Зарарли ҳатти-ҳаракатларни аниқлаш тизимлари (misuse detection) тажовузкорни ҳатти-ҳаракатларини тавсифловчи белгиларнинг олдиндан маълум бўлишига асосланади. Зарарли ҳатти-ҳаракатларни аниқлаш технологиясининг энг кенг тарқалган кўриниши бу эксперт тизимлардир. Масалан, Snort, RealSecure IDS, Enterasys Advanced Dragon IDS тизимлари.

Ушбу тизимларда қўлланиладиган технологияларни батафсил кўриб чиқайлик (1-расм) [10].



1-расм. Мавжуд ҲАТ технологиялари

Аномал фаолиятни аниқлаш технологиялари. Аномалия сенсорлари индивидуал объектни ишлашида аномалия деб аталадиган ноодатий ҳатти-ҳаракатларни аниқлайди. Шунинг учун уларни амалда қўллашда асосий қийинчилик ҳимояланган объектларни ўзлари, шунингдек, улар билан ўзаро таъсир қилувчи ташқи объектларнинг беқарорлиги билан боғлиқ. Кузатув объекти бутун тармоқ, алоҳида компютер, тармоқ хизмати, фойдаланувчи ва бошқалар бўлиши мумкин. Турли хил иловалар кузатилган ҳатти-ҳаракатларнинг рухсат этилганидан рухсат этилган оғишнинг ўзига хос таърифига ва кузатиш сенсорининг "ишлаб кетиш бўсағаси" учун ўз таърифига эга.

Аномалияларни аниқлашда кенг қўлланиладиган чора-тадбирлар ва усулларга қуйидагилар киради [10]:

- бўсаға қийматлар: объект кузатувлари рақамли интерваллар сифатида ифодаланади. Ушбу интерваллардан ташқарига чиқиш аномал ҳатти-ҳаракатлар ҳисобланади. Масалан, кузатилиши мумкин бўлган параметрлар сифатида қуйидагилар бўлиши мумкин: фойдаланувчи маълум вақт оралиғида кирган файллар сони, тизимга киришга муваффақиятсиз уринишлар сони, СПУ юки ва бошқалар. Эшиклар статик ёки динамик бўлиши мумкин;
- параметрик: ҳужумларни аниқлаш учун махсус шаблонларга асосланган "оддий тизим профили";
- параметрик бўлмаган: профил ўқув даврида объектни кузатиш асосида қурилади;
- статистик чора-тадбирлар: ҳужум мавжудлиги тўғрисидаги қарор статистик олдиндан ишлов бериш орқали тўпланган катта ҳажмдаги маълумотлар асосида қабул қилинади;
- қоидага асосланган чора-тадбирлар (сигнатуралар): бу параметрик бўлмаган статистик кўрсаткичларга жуда ўхшаш. Ўқув даврида объектнинг одатий ҳатти-ҳаракати ҳақида ғоя шаклланади, бу махсус "қоидалар" шаклида қайд этилади. Объектнинг "яхши" ҳатти-ҳаракатининг сигнатуралари олинади;
- бошқа чора-тадбирлар: нейрон тармоқлар, сенсор-сенсорга кўринадиган маълум хусусиятлар тўпламини таснифлаш имконини берувчи генетик алгоритмлар.

Замонавий аномалияларни аниқлаш тизимларида биринчи иккита усул асосан қўлланилади. Шуни таъкидлаш керакки, ушбу технологиядан фойдаланишда иккита экстремал мавжуд:

- ҳужум бўлмаган аномал ҳатти-ҳаракатни аниқлаш ва уни ҳужум деб таснифлаш (иккинчи турдаги хато);
- аномал ҳатти-ҳаракат таърифига кирмайдиган ҳужумни ўтказиб юбориш (биринчи турдаги хато). Бу ҳолат ҳужумлар синфига аномал ҳатти-ҳаракатларни нотўғри белгилашдан кўра анча хавфлидир. Шунинг учун, ушбу тоифадаги тизимларни ўрнатиш ва операцион тизимни ўрнатишда оддий фойдаланувчилар ва мутахассислар иккита жуда муҳим бўлмаган вазифага дуч келишади:
- юқорида тавсифланган иккита экстремал ҳолатдан бирининг юзага келиш эҳтимолини камайтириш учун субъэктнинг ҳатти-ҳаракати хусусиятларининг чегара қийматларини аниқлаш;
- объектнинг профилини яратиш - бу расмийлаштириш қийин ва кўп вақт талаб қиладиган вазифа бўлиб, хавфсизлик бўйича мутахассисдан жуда кўп дастлабки ишларни, юқори малака ва тажрибани талаб қилади.

Одатда, аномал фаолиятни аниқлаш тизимлари таҳлил қилиш учун маълумотлар манбаи сифатида журналлар ва жорий фойдаланувчи фаолиятидан фойдаланади. Аномал ҳатти-ҳаракатларни аниқлаш технологиясига асосланган ҳужумларни аниқлаш тизимларининг афзалликлари қуйидагилардан иборат:

- сигнатураларни ва киришни аниқлаш қоидаларини янгилаш шарт эмас;
- сигнатуралари ҳали ишлаб чиқилмаган ҳужумларни янги турларини аниқлашга қодир;
- зарарли ҳатти-ҳаракатларни аниқлаш тизимларида фойдаланиши мумкин бўлган

маълумотларни яратиш.

Ушбу тизимларнинг камчиликлариэса қуйидагилардан иборат:

- кўплаб иккинчи турдаги хатоларни генерация қилиши;
- узоқ муддатли ва сифатли таълимни талаб қилиши;
- одатда жуда секин ишлайди ва кўп ҳисоблаш ресурсларини талаб қилади.

Компютер ҳужумларининг статистик таҳлили. Статистик таҳлил усулларидан фойдаланиш аномал ҳатти-ҳаракатларни аниқлаш технологиясини амалга оширишнинг энг кенг тарқалган тури ҳисобланади. Статистик сенсорлар объектнинг одатий ҳаракати ҳақида турли хил маълумотларни тўплайди ва уни профил шаклида шакллантиради. Бу ҳолда профил объектнинг одатий ҳаракатини тавсифловчи параметрлар тўпламидир. У кузатилаётган объект статистикаси асосида, математик статистика усулларидан фойдаланган ҳолда тузилади.

Профилнинг дастлабки шаклланиши даври ўтади, шундан сўнг объектнинг ҳаракатлари мос келадиган параметрлар билан таққосланади ва агар сезиларли оғишлар топилса, ҳужумни бошлаш учун сигнал берилади. Профил созламаларини умумий гуруҳларга ажратиш мумкин:

- категорик параметрлар (файл номлари, фойдаланувчи буйруқлари, очиқ портлар ва бошқалар);
- рақамли параметрлар (турли хил протоколлар орқали узатиладиган маълумотлар миқдори, процессор юкламаси, фойдаланилган файллар сони ва бошқалар);
- олдинги турдаги параметрлар билан бир қаторда таснифга мос келмайдиган.

Объектнинг ўзгарувчан ҳатти-ҳаракатларини тўлиқроқ тасвирлаш учун профилларда динамик ўзгариш механизмлари ҳам мавжуд. Статистик усуллардан фойдаланадиган тизимлар бир қатор афзалликларга эга:

- ҳужум сигнатуралари маълумотлар базасини доимий янгилашни талаб қилманг (бу ушбу тизимларни сақлаш вазифасини сезиларли даражада осонлаштиради);
- фойдаланувчи ҳатти-ҳаракатларининг ўзгаришига мослаша олади ва шунинг учун одамларга қараганда ҳужумчилик уринишларига нисбатан сезгирроқдир;
- сигнатуралари ҳали ёзилмаган номаълум ҳужумларни аниқлай олади ва шунинг учун эксперт тизимлари учун тегишли шаблон ишлаб чиқилгунга қадар ўзига хос буфер вазифасини бажаради;
- Бошқа усулларга қараганда мураккаброқ ҳужумларни аниқлаш имконини беради, масалан, вақт ўтиши билан ёки ҳужум объектлари томонидан тақсимланади.

Ҳужумларни аниқлаш тизимларининг камчиликлари орасида қуйидагилар мавжуд:

- статистик усулларда ҳужум ҳақида ёлғон хабарларни олиш эҳтимоли бошқа усулларга қараганда анча юқори;
- чегара қийматини ўрнатишнинг қийинлиги (бу қийматларни танлаш бошқариладиган тизимни чуқур билишни талаб қиладиган жуда аҳамиятсиз вазифадир);
- статистик усуллар фойдаланувчи фаолиятидаги ўзгаришларни унчалик тўғри кўриб чиқа олмайди (масалан, бошқарувчи танқидий вазиятда бўйсунувчи сифатида ҳаракат қилганда). Бу камчилик тез-тез ўзгариб турадиган ташкилотларда катта муаммо бўлиши мумкин. Натижада, ҳам ёлғон хавф ҳисоботлари, ҳам салбий нотўғри ҳисоботлар (ўтказиб юборилган ҳужумлар) пайдо бўлиши мумкин;
- тизим, агар иш режимидаги ўзгаришлар аста-секин бўлса, янги ҳатти-ҳаракатларга мослашиши туфайли ҳужумга мос келадиган фаолиятни нормал деб қабул қилиши мумкин;
- статистик усуллар одатий ҳатти-ҳаракатлар намунасини тасвирлаб бўлмайдиган субъэктларнинг ҳужумларини аниқлай олмайди;
- статистик усуллар олдиндан тузилган бўлиши керак (ҳар бир параметр, ҳар бир фойдаланувчи учун чегара қийматлари ўрнатилади);
- фақат статистик усулларга асосланган тизимлар рухсат этилмаган ҳаракатларни амалга оширадиган субъэктларнинг ҳужумларини бошиданоқ аниқлашга дош бера олмайди, чунки улар учун одатий ҳатти-ҳаракатлар намунаси фақат ҳужумларни ўз ичига олади;

- профилга асосланган статистик усуллар воқеалар тартибига бефарқ.

Бироқ, бу муаммоларни ҳал қилишнинг йўллари мавжуд ва уларни амалда қўллаш фақат вақт масаласидир. Шубҳасиз, статистик усул аномал ҳатти-ҳаракатлар технологиясини соф амалга оширишдир. Статистик усул аномалияларни аниқлаш технологиясидан амалда зарур бўлган барча афзалликларни мерос қилиб олади [11].

Ҳужумларни аниқлашнинг замонавий тизимлари камчиликлари. Юқоридагилардан келиб чиққан ҳолда, барча ҳужумларни аниқлаш тизимларини қидирувга йўналтирилган тизимларга бўлиш мумкин:

- барча таниқли ҳужумларнинг сигнатуралари;
- бошқариладиган объектларнинг ўзаро таъсиридаги аномалиялар;
- эталонлар профили маълумотларини бузиш.

Ҳозирги вақтда гибрид тизимлар, шунингдек, вақт ва маконда тақсимланган маълумотлардан фойдаланадиган тизимлар деярли йўқ. Замонавий тизимларни кўпчилиги ишлаши давомида фақат ҳужум таъсирини таниб олиш ёки бошқариладиган тармоқ ҳатти-ҳаракатларидаги аномалияларни қидиришда сигнатура усули қўлланилади. Бундан ташқари, деярли барча маълум тизимларда ҳужум симулятори ёки жойлаштирилган ва бошқариладиган СОА нинг тўғрилигини текшириш учун бошқа воситалар мавжуд эмас, бу ҳар бир аниқ компютер тармоғида фойдаланиладиган конфигурация параметрларини текширишнинг оддий ва ишончли воситасини таъминлайди. Ушбу восита, мантиқий сабабларга кўра, вирус типидаги дастурий таъминот, хизмат кўрсатишни рад этиш ҳужумлари фаолиятини симуляция қилиши керак. Ҳисоб қайдномалари ҳуқуқларини оширишга қаратилган ҳужумлар трафикни қайта йўналтириш ва нотўғри маълумотларни киритиш ҳужуми кабилардир. Буларнинг барчаси билан дастурий таъминот воситаси тақсимланган характердаги ҳужумларни яратиш қобилиятига эга бўлиши мақсадга мувофиқдир.

Масалан, СОА симуляторларининг баъзи турлари архитектураси ҳужумни аниқлаш бўйича кичик вазифаларни ҳал қилиш учун ихтисослашган ҳар хил турдаги агентлар тўпламидан иборат. Агентлар тизимдаги алоҳида компютерларда жойлашган. Ушбу архитектурада агентлар оиласи учун аниқ "назорат маркази" мавжуд эмас, чунки вазиятга қараб, ҳамкорлик ва назорат функцияларини бошлайдиган ҳар қандай агент этакчи бўлиши мумкин. Агар керак бўлса, уларни тармоқ ва локал муҳитда нусхалаш ёки ишлашни тўхтатиш мумкин. Вазиятга кўра ҳар бир синф агентларининг бир нечта нусхаларини яратиш керак бўлиши мумкин. Тизим архитектураси тўпланган тажрибадан фойдаланган ҳолда тармоқни қайта конфигурацияга, трафик ўзгаришларига ва янги турдаги ҳужумларга мослаша олади.

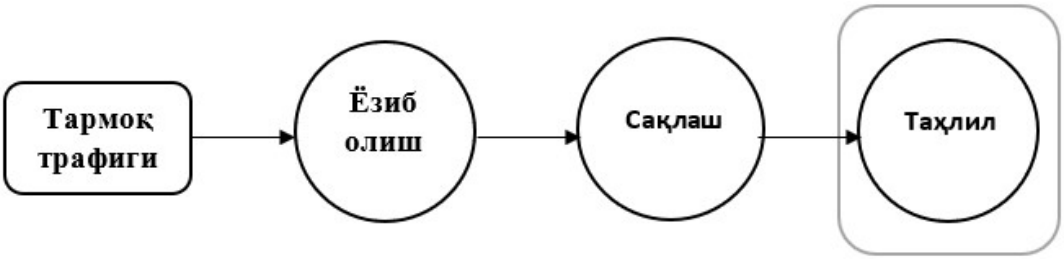
Кўп агентли тизимлар қизиқарли ишланмадир, аммо локал ишларда ҳужумни аниқлаш алгоритмлари ишлатилган ёки ишлаб чиқилганлиги ҳақида ҳеч қандай кўрсатма йўқ. Бундан ташқари, таниқли симуляторларнинг жорий версиялари реал вақтда ишламайди, чунки танланган асосий воситалар тўплами бунга рухсат бермайди.

Умуман олганда, СОА самарадорлигини баҳолаш учун ҳужум симуляторларининг етишмаслиги бу йўналишдаги асосий муаммо эмас. Мавжуд аниқлаш тизимларининг ҳақиқий камчиликлари оддий сигнатура излашнинг примитивлиги, вақт ва жойда тақсимланган мураккаб ҳужумларни аниқлашнинг паст самарадорлиги, қўшма ҳужумлар ва рухсат этилмаган киришларни аниқлаш учун хост ва тармоқ даражасидаги маълумотларнинг етарли даражада интеграцияланмаганлиги.

Операцион камчиликлар сифатида ҳодисанинг тегишлилигини "дўст ёки душман" га бўлиш учун жуда кўп ҳисоблаш операцияларини ва барча кирувчи маълумотларни оддий шахсий компютерларда реал вақт режимида қайта ишлашнинг мумкин эмаслигини қайд этиш мумкин, чунки тармоқни қайта ишлаш тезлиги ёки бошқа ҳодисалар трафиги кўпинча реал вақтда реал вақтга қараганда 1,5-2 марта секинроқ. Шунинг учун баъзи тизимларда таҳлил кечиктирилган режимда содир бўлади. Бунда ҳимояланган ахборот ва ҳисоблаш ресурсларига ҳужум ўз вақтида сезилмайди ва ундан ҳам кўпроқ мавжуд ҳимоя воситаларидан фойдаланган ҳолда акс эттирилмайди. Ушбу режимда ҳужумни аниқлаш воситаларидан кейинги текшириш учун ҳужумнинг барча босқичларини қайд қилиш воситаси сифатида фойдаланиш мумкин.

Аксарият замонавий СОАлар дастлаб турли хил операцион тизимлар ва ихтиёрий аппарат ва ҳисоблаш платформаларида ишлаш учун мўлжалланмаган. Шунинг учун, кўпгина маҳсулотлар учун бир нечта операцион тизимларда ишлаш мумкин эмас. Ушбу тизимлар танланган операцион тизимлар ва аппарат платформалари учун кодни ишлаб чиқиш ва оптималлаштиришдан фойдаланмайди, бу уларнинг энг муҳим камчиликларидан биридир. Шунингдек, бирон бир дастурий таъминот ёки аппарат-дастурий таъминот тизими асосий комплекс ишламай қолган тақдирда заҳиравий комплексни тезда ишга тушириш ва вайрон қилинган мудофаа чизиғини тиклаш имконини берадиган "иссиқ алмаштириш" режимини таъминламайди. Шунга қарамай, аномалияларни аниқлаш тизимларини ишлаб чиқишда ижобий момент мавжуд - бу ишлаб чиқувчиларнинг ўз тизимларини мавжуд ҳимоя воситалари билан интеграция қилиши ҳисобланади.

Тизимни лойиҳалаш. Таҳлил тизими трафикни 100% ни эгаллаши ва натижалар бўйича навигация билан самарали таҳлил усулларини таъминлаши керак. Агар тармоқ трафигини таҳлил қилиш муаммосини комплекс ҳал қилиш ҳақида гапирадиган бўлсак, унда биринчи навбатда уни учта мустақил кичик вазифага бўлиш керак (2-расм): трафикни тутиб олиш, сақлаш ва таҳлил қилиш [12].



2-расм - Тармоқ трафигини таҳлил қилиш тизимининг қуйи вазифалари

Трафикни тутиб олиш масаласи. Трафикни ушлаш снифферлар ёрдамида амалга оширилади. Умуман олганда, сниффер трафикни тутиб олиш учун мўлжалланган дастур ёки дастурий-аппарат қурилмасидир. Муайян маҳсулотларда қўшимча функциялар амалга оширилиши мумкин, масалан, тармоқ протоколи сарлавҳаларини таҳлил қилиш, белгиланган мезонлар бўйича филтрлаш, сессияни тиклаш. Тармоқ трафигини тутиб олиш қуйидаги ҳолларда амалга оширилиши мумкин:

- тармоқ интерфейсида "тинглаш" орқали;
- снифферни канал узилишига улаш;
- траффикни тармоққа бўлиш ("кўзгулаштириш") ва унинг нусхасини снифферга юбориш (мисол: Network tap);
- сохта электромагнит нурланишни таҳлил қилиш орқали;
- ҳавола ёки тармоқ даражасидаги ҳужум орқали, жабрланувчининг трафигини снифферга йўналтиришга олиб келади.

Жойлашувига кўра, снифферлар икки хил бўлади:

- маршрутизаторда (шлюз);
- тармоқнинг охирги тугунида.

Биринчи ҳолда, қурилма интерфейслари орқали ўтадиган барча трафик тўхтатилади, иккинчидан - агар тармоқ картаси нормал режимда ишлаётган бўлса, фақат тармоқ тугунининг трафигини ёки ушбу тармоқ сегментининг барча қурилмалари пакетларини ушлаб туради (бунинг учун тармоқ картаси "promiscuous" режимига ўтказилади - ўқиб бўлмайдиган). Бундай дастурлар эркин тақсимланган Pcap кутубхонаси (инглизча "packet capture") асосида яратилган. У C/C++ тиллари билан биргаликда фойдаланиш учун мўлжалланган ва ўрамлардан Java, .NET каби бошқа тилларда кутубхона билан ишлаш учун фойдаланилади. Unix-га ўхшаш тизимлар учун бу libpcap кутубхонаси ва Microsoft Windows учун – WinPcap.

Тармоқ мониторинги дастури тармоқдаги пакетларни олиш, тармоқдаги пакетларни узатиш учун libpcap ёки WinPcap -дан фойдаланиши мумкин. Шунингдек, у олинган

пакетларни файлга сақлашни ва сақланган пакетларни ўз ичига олган файлларни ўқишни қўллаб-қувватлайди.

Таклиф этилаётган тизим мос равишда провайдер тармоғини ва интернетни боғлайдиган чиқиш йўриқномасига уланганлиги сабабли, қайта ишланган трафикнинг бундай ҳажмига эга ускунанинг ишлашида кечикишлар яратмаслик учун трафикни "аксилаш" усулдан фойдаланилди (3-расм).

3-расм - Ахборот йиғиш тизимини ўрнатиш схемаси

Трафикни таҳлил қилиш масаласи. Таҳлил вазифасига келсак, ҳал қилиниши керак бўлган кичик вазифаларнинг ўзига хос хусусиятларидан келиб чиққан ҳолда у ёки бу воситага устунлик берилади [11]. Мавжуд ускуналарнинг аксарияти, қоида тариқасида, тармоқ протоколи сарлавҳаларини таҳлил қилади, шунингдек, сессияларни тиклайди (асосий таҳлил). Шу билан бирга, жуда аниқ вазифалар мавжуд, улар учун тайёр восита бўлмаслиги мумкин, масалан:

- ихтиёрий чуқурликдаги туннеллаш протоколларини таҳлил қилиш;
- амалий даражадаги сеансларни таҳлил қилиш (тармоқ орқали узатиладиган маълумотлар оқими ўртасидаги боғлиқларни аниқлаш);
- трафикда олдиндан белгиланган сигнатуралар аниқланган тақдирда муайян сценарийларни (скриптларни) бажариш.

Анализаторларнинг иккита иш режими мавжуд:

- реал вақтда;
- олдиндан сақланган трафик бўйича.

Реал вақтда таҳлил қилиш ускунани доимий режимда қўллаб-қувватлашни, киришга кирувчи трафикни таҳлил қилиш учун этарли ишлашни талаб қилади. Бундай ҳолда, потенциал чексиз кириш маълумотлар оқимини қайта ишлаш имконияти бўлиши керак.

Қолдирилган таҳлил бўлса, ускуна файлдан кириш маълумотларини олади, бу эса шунга ўхшаш трафик бўйича реал вақт таҳлилига нисбатан тармоқ йўналишини батафсилроқ таҳлил қилиш имконини беради.

Ишни тахминий баҳолаш ва тизим прототипини синовдан ўтказиш учун бизга канал кенглиги 1,5 Гбит/с бўлган "Тошкент Ирригация ва қишлоқ хўжалигини механизациялаш муҳандислари институти" миллий тадқиқот университети трафигини тақдим этдик. Агар 2021

йил 31-май ҳолатига кўра трафик статистикаси маълумотларига қаралса (1-жадвал), жами унинг ўртача юкланиши 633,1 Мбит/с ни ташкил қилади. Шунга кўра, бундай оқимни реал вақтда қайта ишлаш қийин. Бу трафикни сақлаш муаммосини ҳал қилиш зарурлигини англатади.

1-жадвал. Кунлик трафик статистикаси

Канал	Максимал канал юки (Мб/с)	Ўртача юклаш (Мб/с)	Жорий юк (Мб/с)
Кирувчи	920.2	510,8	610,7
Чиқувчи	302.7	122.3	160.5

Трафикни сақлаш масаласи. Тўпламни қайта ишлаш ва ўзгартириш эгаллаган жойни қисқартириш ва маълумотлар намуналарини оптималлаштириш учун зарурдир. Бунга эришиш учун маълумотлар базалари жуда мос келади. Биринчидан, бу бутун тўпламдаги шартларга мос келадиган пакетларни тезда топиш имкониятини беради, чунки уларнинг ҳар бири жадвалда алоҳида ёзув сифатида сақланади. Бундан ташқари, индекслаш катта ҳажмдаги маълумотларни танлашни тезлаштириш учун ишлатилади.

Индекс - бу жадвалнинг бир ёки бир нечта устунлари қийматлари ва жадвалдаги тегишли сатрларга кўрсатгичлардан яратилган маълумотлар базаси объекти. Шунга кўра, ишнинг тезлашиши, биринчи навбатда, индекс қидирув учун оптималлаштирилган тузилишга эга бўлганлиги сабабли эришилади.

Индексларнинг икки тури мавжуд: кластерли ва кластерсиз. Агар кластерли индекс мавжуд бўлса, жадвал сатрлари индекс калит қиймати бўйича тартибланади.

Агар жадвалда кластерли индекс бўлмаса, жадвал тўп деб аталади ва бундай жадвал учун яратилган индекс фақат ёзувларга кўрсатгичларни ўз ичига олади. Бу индексларнинг иккинчи тури. Ҳар бир жадвалда фақат битта кластерли индекс бўлиши мумкин, лекин ҳар бир жадвалда бир нечта кластерланмаган индекслар бўлиши мумкин, уларнинг ҳар бири ўзининг рекорд тартибини белгилайди.

Сўровларнинг оптимал ишлаши учун индекслар одатда сўровларда энг кўп ишлатиладиган жадвал устунларида яратилади. Яъни, битта жадвал учун бир нечта индекслар яратилиши мумкин. Бироқ, индекслар сонининг кўпайиши жадвал қаторларини қўшиш, янгилаш, ўчириш операцияларини секинлаштиради, чунки индексларнинг ўзи янгиланиши керак. Улар қўшимча хотирани эгаллаганлиги сабабли, уларни яратишдан олдин, сўровлар учун кутилган самарадорлик индексни сақлаш учун компютер ресурсларининг қўшимча харажатларидан устун бўлишига ишонч ҳосил қилишингиз керак.

Иккинчидан, маълумотлар базаларидан фойдаланиш эгалланган майдон ҳажмини камайтиришни таъминлаши керак, чунки яхши ўйланган архитектурада фақат рўйхатдан ўтган маълумотлар сақлаш учун қолади.

Ишлаб чиқилган прототипда 200 ГБ ҳажмдаги университет трафиги айлантирилди ва маълумотлар базасида қайд этилди; янги маълумотларнинг ҳажми 134,4 Гб ни ташкил этди, бу 1,5 марта сиқишни кўрсатади. Рўйхатга олинган пакетлар сони 142 млн. Шундай қилиб, тизимни ишга туширишдан олдин, тадқиқот ўтказиш керак, яъни қайси маълумотлар базалари бу мақсад учун энг мос келади.

2 Хулоса

Рухсат этилмаган таъсирлардан ҳимоя қилиш учун тармоқ трафигини таҳлил қилиш муаммосининг долзарблигини асослайди ва ушбу муаммони ҳал қилишнинг мавжуд усулларини кўриб чиқади.

Сўнгги пайтларда бошқарув тизимлари соҳасида иккита аниқ тенденция кузатилди:

- тармоқлар ва тизимларни бошқариш функцияларини бир маҳсулотга бирлаштириш;
- қурилмалар ва қуйи тизимларнинг ҳолати тўғрисида маълумот тўплайдиган ва кейин бошқарув ҳаракатларини чиқарадиган бир нечта консоллар мавжуд бўлган бошқарув тизимини тақсимлаш.

Бунинг сабаби шундаки, тақдим этилган тизимларнинг аксарияти юқори даражада ихтисослашган ва уларнинг функтционал имкониятларини яхши бажаришга қаратилган. Шунга кўра, мутахассислар тармоқнинг барча мумкин бўлган заифликларини тўлиқ қоплаш учун бир нечта маҳсулотлар тўпламидан фойдаланишлари керак: трафикни кузатиш ва ҳисобга олиш тизимлари ускуналар ва тармоқнинг ишлашини текширади, жорий аппарат ва дастурий таъминот конфигурациясининг оптималлигини аниқлайди; тажовузларни аниқлаш ва олдини олиш тизимлари - тармоқ ичида ва ташқарисида таҳдидни аниқлаш имконини беради.

Тармоққа тажовузларни аниқлаш тизимларини яратиш ва ахборот тизимларига компютер ҳужумлари белгиларини аниқлашнинг замонавий ёндашуви камчиликлар ва заифликларга тўла бўлиб, улар, афсуски, зарарли таъсирларнинг ахборотни ҳимоя қилиш чегараларини муваффақиятли энгиб ўтишга имкон беради.

Прототипнинг архитектураси ишлаб чиқилган ва тизимнинг қуйидаги модуллари тавсифланган:

- трафикни қайд этиш модули;
- пакетни сақлаш модули;
- маълумотларни таҳлил қилиш модули.

Айрим модуллар учун ҳам муҳим мезонлар аниқланди. Мисол учун, трафикни тутиб олишда "кўзгулаштириш" усулидан фойдаланиш, дампни айлантириш ва маълумотлар базасига сақлаш кераклигини аниқланди.

Адабиётлар

[1] Мустафаев, А. Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика: http://e-notabene.ru

[2] Анализ угроз сетевой безопасности: http://ypn.ru

[3] Басараб, М. А. Анализ сетевого трафика корпоративной сети университета методами нелинейной динамики: М. А. Басараб, А. В. Колесников, И. П. Иванов // Наука и образование: научное издание / МГТУ им. Н. Э. Баумана.: http://technomag.bmstu.ru/doc/587054.html.

[4] Cecil Alisha. A Summary of Network Traffic Monitoring and Analysis Techniques: http://www.cse.wustl.edu

[5] Олифер, Н. А. Средства анализа и оптимизации локальных сетей: http://citforum.ru

[6] Чивчалов, А. Shodan – самый страшный поисковик Интернета: https://habrahabr.ru/post/178501/

[7] IDS/IPS — Системы обнаружения и предотвращения вторжений: http://netconfig.ru

[8] IDS/IPS - системы обнаружения и предотвращения вторжений и хакерских атак: http://www.altell.ru

[9] Лукацкий, А. Предотвращение сетевых атак: технологии и решения: http://citforum.ru/security/articles/ips/.

[10] Новый подход к защите информации – системы обнаружения компьютерных угроз: http://www.jetinfo.ru

[11] Михеев, А. В. Исследование методов сбора статистических данных о трафике в ip-сетях передачи данных: статья / А. В. Михеев // электронный научный архив Уральского федерального университета им. Б. Н. Ельцина: http://elar.urfu.ru

[12] Маркин, Ю. В. Обзор современных инструментов анализа сетевого трафика: статья / Ю. В. Маркин, А. С Санаров // сборники трудов Института системного программирования Российской академии наук: http://www.ispras.ru/preprints

22.04.2022 да таҳририятга келиб тушган

UDC 004.95

DEVELOPMENT OF NETWORK TRAFFIC ANALYSIS SYSTEM

[1]Abdullaeva B.M., [2]Samijonov B.N., [3]Erejepov K.K., [1]Jo'raeva M.A., [1]Abduvaxobov F.F.

[1]Namangan State University,
160107, 161, Boburshoh, Namangan, Uzbekistan;
[2]Inha University in Tashkent,
100170, 9, Intellectuals, Tashkent, Uzbekistan;
[3]Tashkent university of information technologies named after
Muhammad al-Khwarizmi, Nukus branch,
230101, 74, A. Dosnazarov, Nukus, Uzbekistan.

This article discusses the development of a prototype system for collecting network traffic to analyze and detect unauthorized activity, as well as the functionality of the system to receive, store, process and visualize network traffic from the local network to the external Internet.

During the work, modern methods of network traffic analysis were studied, system architecture was developed, statistical traffic processing algorithms were created, and system performance was tested on real data obtained from the network. The system prototype connects to the network infrastructure near the output router and allows the traffic packet to be processed to present its statistics in a convenient form.

Keywords: network, traffic, system, data, prototype, visual, attack.

Citation: Abdullaeva B.M., Samijonov B.N., Erejepov K.K., Jo'raeva M.A., Abduvaxobov F.F. 2022. Development of network traffic analysis system // *Problems of Computational and Applied Mathematics.* 2/1(40): 19-30.