UOT 004.49;004.056

KOMPÜTER ŞƏBƏKƏLƏRİNƏ HÜCUMLARIN AŞKARLANMASI ÜSULLARININ TƏSNİFATI

dosent Məmmədov Məhil İsa oğlu, Hüseynova Dilkəş Bəxtiyar qızı,
Əliyeva Aytən Natiq qızı, Məmmədova Sima Kəmaləddin qızı
Azərbaycan Dövlət Aqrar Universiteti
gceferova@rambler

Xülasə:*Müasir dövrümüzdə informasiya-kommunikasiya texnologiyalarının, xüsusilə də kompüter şəbəkələrinin sürətli inkişafı yeni yanaşmalar tələb edən şəbəkə ehtiyatlarının təhlükəsizliyi ilə bağlı bir sıra problemlər yaradır. Hazırda hücumların aşkarlanması sistemlərinin qurulması məsələləri şəbəkə texnologiyaları sahəsində aktual istiqamətdir.*

Məqalədə şəbəkə hücumlarının aşkarlanması və təsnifatı üçün əsas metodların təhlili verilmiş, bu metodların təsnifatının ümumiləşdirilmiş sxemi təklif olunur.

Məqalədə şəbəkə hücumlarının aşkarlanmasının müxtəlif metodları nəzərdən keçirilir. Əsas diqqət şəbəkə hücumlarının aşkarlanması metodlarının ümumiləşdirilmiş təsnifat sxeminin qurulmasına, nəzərdən keçirilən metodların hər birinin mahiyyətinin təqdim edilməsinə və onların təklif olunan təsnifat sxemi çərçivəsində müqayisəli təhlilinə yönəldilir.

Açar sözlər. şəbəkə hücumları, sui-istifadə aşkarlanması, anomaliyaların aşkarlanması, şəbəkə trafiki.

Keywords: network attacks, abuse detection, anomaly detection, network traffic.

Ключевые слова: сетевые атаки, обнаружение злоупотреблений, обнаружение аномалий, сетевой трафик.

Elektron vasitələrdən istifadə etməklə həyata keçirilən informasiya hücumlarının artması ilk növbədə, İnternetin yayılması ilə sıx bağlıdır. Kompüter və şəbəkə texnologiyalarından istifadə etməklə bir neçə saniyə ərzində müxtəlif məxfi məlumatlar yerləşdiyi məkandan asılı olmayaraq oğurlanır, nəzarətdə saxlanılır və ya məhv edilir. Kompyuter şəbəkəsindən istifadə etməklə həyata keçirilən bu əməliyyatların transmilli xarakter alması belə deməyə əsas verir ki, informasiya hücumları ilə mübarizədə istənilən strategiyanın əsas hissəsi problemlərin həlli ilə əlaqədar ümumi siyasətin işlənməsidir [1]. Kompüter şəbəkələrinin və informasiya texnologiyalarının sürətlə inkişafı yeni yanaşmalar tələb edən şəbəkə ehtiyatlarının təhlükəsizliyi ilə bağlı bir sıra problemlərə səbəb olur. Hazırda hücumların aşkarlanması sistemlərinin qurulması məsələləri informasiya texnologiyaları sahəsində aktual istiqamətdir. Məlumatların intellektual təhlili metodlarının tətbiqi ilə siqnal nümunələrinə uyğunluq əsasında ənənəvi yanaşmalar və adaptiv modellər daxildir. Bu işlərin əksəriyyəti kifayət qədər uzun müddətdir ki, onların bəziləri yalnız konkret fənn haqqında, yəni sui-istifadə və ya anomaliyaların aşkar edilməsi şəklində böyük həcmli aspektə malikdirlər[2].

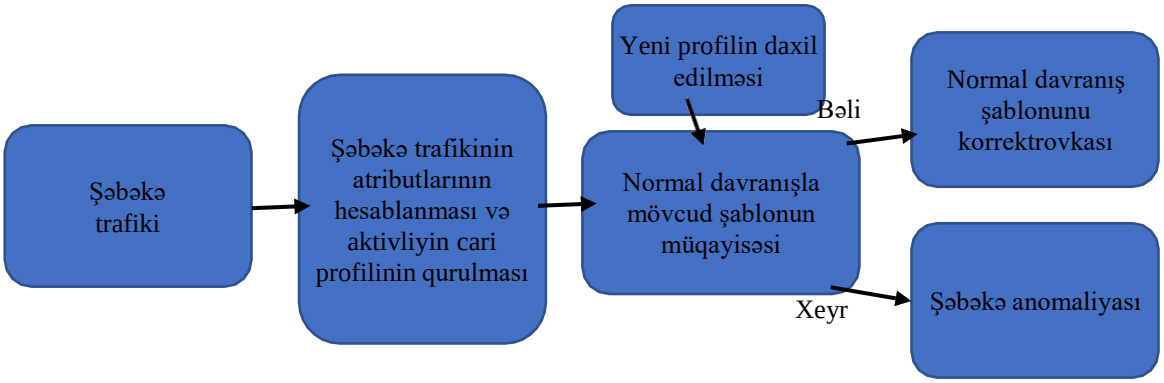
Hücumların aşkarlanması üsullarının təsnifatı sxemi. Hücumların aşkar edilməsi üsulları üzrə hücum aşkarlama sistemlərinin ümumi qəbul edilmiş təsnifatı anomaliyaların aşkarlanması sistemləri və sui-istifadənin aşkar edilməsi sistemlərini ehtiva edir. Kompüter şəbəkələrinin normal işinin təmin edilməsi məqsədilə şəbəkə hücumlarının qarşısının alınması üçün standart qoruma vasitələri (məsələn, ŞE, ehtiyat surətin saxlanılması sistemi, antivirus proqramları) ilə yanaşı reallaşdırılması zəruri olan əsas vasitələrdən biri də hücumların aşkarlanması sistemləridir [2].

Hücumların aşkarlanması sistemlərinin nümunəvi arxitekturasına, bir qayda olaraq, aşağıdakı komponentlər daxil olur:

- informasiyanın toplanması vasitələri – sensor;
- informasiyanın təhlili vasitələri – analizator;
- reaksiyavermə vasitələri;

- idarəetmə vasitələri.

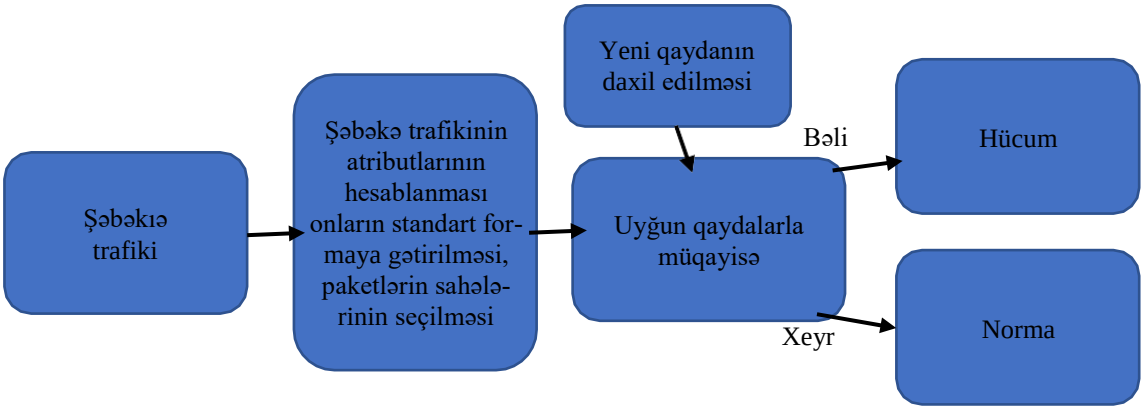
Şəbəkə hücumlarının aşkarlanması üsulları iki əsas qrupa bölünür: anomaliyaların aşkarlanması üsulları və sui-istifadə aşkar üsulları [3]. Şəkil 1-də şəbəkə trafikinin göstəriciləri əsasında şəbəkə anomaliyalarının aşkarlanması sxemi göstərilir.



Şək. 1. Şəbəkə anomaliyalarının aşkarlanması sxemi

Şəbəkə anomaliyalarının aşkarlanmasının ümumi alqoritmi aşağıdakı kimi təsvir edilə bilər. Analiz üçün verilənlər ümumi halda IP səviyyəsində parçalanmış şəbəkə paketlərinin dəsti kimi təqdim olunan şəbəkə trafikidir. Toplanmış ilkin məlumatlar sonrakı təhlil üçün zəruri məlumatların formalaşmasında mənbə kimi xidmət edəcək. Belə ki, əldə edilən məlumatlar müəyyən bir zaman aralığında aqreqasiya edilə bilər və cari fəaliyyət profilinin qurulmasında tələb olunacaq ümumi növün əlamətdar atributlarını tapşırmaq məqsədilə normallaşdırıla bilər. Obyektin (istifadəçinin və ya sistemin) normal fəaliyyətinin xarakteristikaları toplusu - normal davranış şablonu ilə müqayisə olunur. Əgər müqayisə olunan parametrlərin əhəmiyyətli dərəcədə fərqlənməsi müşahidə olunursa, onda şəbəkə anomaliyası qeydə alınır. Əks təqdirdə, şəbəkə fəaliyyətinin mövcud müşahidə olunan profilini nəzərə alaraq, onun parametrlərini dəyişdirməklə normal davranış şablonu dəqiqləşdirilir [3].

Yuxarıda təsvir olunan alqoritm normal davranış şablonuna uyğunluğunu yoxlamaq üçün alt sistemin həyata keçirilməsi üçün bir neçə icra variantını əhatə edə bilər. Onların ən sadəsi, cari şəbəkə aktivliyini təsvir edən toplanan nəticələrin ekstremal olaraq verilmiş nömrəli çubuqla müqayisə olunması ilə müqayisə prosesi-axmaqlığıdır. Bu yanaşmada göstərilən sərhədin nəzərdən keçirilən parametrlərinin həddindən artıq olması şəbəkə anomaliyasının əlamətidir.



Şəkil 2-də şəbəkə trafikində düzgün istifadə edilməməsinin sxematik diaqramını göstərir[3].

Şəkil: 2. Şəbəkədən sui-istifadə aşkarlama sxemi

Sui-istifadə aşkarlanması icazəsiz hərəkətləri, əgər onların hücum şablonları şəklində dəqiq təsəvvürü varsa, müəyyənləşdirməyə imkan verir. Burada hücum şablonu dedikdə, müəyyən hücumu (müqayisə qaydalarını, çıxarılma qaydalarını) açıq şəkildə təsvir edən bəzi hərəkətlərin məcmusu başa düşülür. Şəbəkə anomaliyalarının aşkar edilməsi sxemində olduğu kimi, analiz üçün ilkin məlumatlardan sui-istifadə aşkar edildikdə şəbəkə trafikidir. Seçilmiş atributlar və şəbəkə paketlərinin sahələri giriş məlumatlarının qaydalara uyğunluğuna dair axtarış və yoxlama aparan və qaydalardan birinin müsbət işlədilməsi halında təhlükənin mövcudluğunu bildirən modula ötürülür.

Hər hansı bir sui-istifadənin aşkarlanması sisteminin yaradılması zamanı əsas problem qaydaların tapşırıq mexanizminin effektiv layihələndirilməsi məsələsidir. Aydındır ki, müxtəlif hücumların aşkarlanması üçün hərtərəfli qaydalar bazasının yaradılması bir neçə amilə görə mümkün deyil. Bu amillərdən biri də ondan ibarətdir ki, hücum hərəkətlərinin müxtəlif variasiyalarının təsviri sistemin məhsuldarlığına mənfi təsir göstərir. Hücumda baş verən mühüm dəyişikliklər belə, sui-istifadə üsullarının aşkar edilməsinin mümkünsüzlüyünə gətirib çıxardığından, verilən qaydalar universal olmalı və şəbəkə hücumlarının mümkün qədər çox tanınmış modifikasiyalarını əhatə etməlidir.

Deyilənləri yekunlaşdıraraq qeyd edək ki, sui-istifadənin aşkarlanması metodları məlum hücum növlərini müəyyən etmək üçün effektiv vasitədir, lakin onların yeni hücumlara, eləcə də məlum hücumların modifikasiyası ilə əlaqədar tətbiq edilməsi nəticəsizdir.

Davranış metodları. Davranış üsulları - informasiya hücum modellərinə deyil, IS-nin "normal" fəaliyyət göstərməsi modellərinə əsaslanır. Bu üsullardan hər hansı birinin işləmə prinsipi informasiya sisteminin mövcud iş rejimi ilə bu IS üçün etalon olan iş rejimi arasındakı fərqlərin aşkar edilməsindən ibarətdir. Hər hansı uyğunsuzluq istila və ya anomaliya kimi nəzərdən keçirilir. Bu prinsipin mürəkkəbliyi informasiya sisteminin "normal" rejiminin dəqiq etalon modelinin yaradılmasıdır.Bu üsullar ilk növbədə istifadəçilərin bir çox legitim hərəkətlərinin dəqiq və tam təsviri ilə izah olunan saxta işlərin olması ilə səciyyələnir [4].

Davranış metodunun qüsurları: istifadəçilərin gözlənilməz davranışlarında saxta siqnallar; gözlənilməz şəbəkə aktivliyi ilə yalançı işləmələr; sistemin tədris mərhələsində müvəqqəti xərclər.

Hər prinsipin bu prinsiplər əsasında qurulmuş öz metodları var [4].

Bu məqalədə aşağıdakı hücum aşkarlama metodları davranış metodları kimi təsnif edilmişdir [2]:

- veyvlet analizi;

- statistik analiz;
- entropiyanın analizi;
- spektral analiz;
- fraktal analiz;
- klaster analizi.

Biliklərə əsaslanma metodları. Bilik əsaslı metodlara belə metodlar daxildir ki, bu metodlar verilmiş faktlar kontekstində, verilən hücumların əlamətlərini əks etdirən çıxarılma və müqayisə qaydaları kontekstində tapılan axtarış mexanizmi əsasında hücumların aşkarlanması üçün hərəkətlər edir [3]. Axtarış proseduru olaraq nümunə üzrə müqayisə, müntəzəm ifadə aparatı, məntiqi sekvensial (ardıcıllığa əsaslanan) nəticə, vəziyyət keçidinin təhlili və s. tətbiq edilə bilər. Bu üsulların adlarından da aydın olur ki, onların tətbiqinə əsaslanan sistemlər artıq məlum olan hücumların təsvirlərini daxil edən bilik bazası ilə işləyir. Burada bilik bazası onların emalı və şərhinin məntiqini dəstəkləyən ekspertlərin qeydlərini ehtiva edən anbar (yəni məntiqi çıxış alt sisteminin olması ilə səciyyələnir) ilə təmsil olunur [5].

Biliklərə əsaslanan metodlara bunları nümunə göstərmək olar:

-siqnalların təhlili üsulu;

-ssenarilərin təsviri dilləri metodu;

-son avtomatlar metodu;

Maşın təlimi metodları. Maşın tədrisi üsulları, həm hesablama intellekti üsulları həm anomaliyaların aşkarlanmasında, həm də sui-istifadə aşkarlanmasında tətbiq olunur. Bu onunla izah olunur ki, bu yanaşmalar təlim üçün mənbə məlumatı kimi çox vaxt şəbəkədə həm normal, həm də anormal davranış şablonlarından istifadə edir [3].

Intellektual hesablama metodları. Süni neyron şəbəkəsi sinapslarla əlaqəli və giriş dəyərlərini istənilən çıxış dəyərləri toplusuna çevirən emal elementləri - neyronlar toplusudur. Neyron şəbəkələr geniş tətbiqlər: obrazların tanınması, idarəetmə nəzəriyyəsi, kriptoqrafiya, məlumatların sıxılması. Neyron şəbəkələr səs-küylü və tam olmayan məlumatlardan ibarət nümunə və ümumiləşdirmə qabiliyyətinə malikdirlər. Təlim prosesində sinaptik tərəzi ilə əlaqələndirilmiş əmsallar tənzimlənir [3].

Hibrid üsullar. Hibrid yanaşmaların varlığı əsas təsnifatçıların birləşdirilməsinin müxtəlif sxemlərinin həyata keçirilməsindən ibarətdir ki, bu da onların ayrı-ayrılıqda fəaliyyət göstərməsindəki qüsurları bərabərləşdirməyə imkan verir. Əsas təsnifatçıların çıxış dəyərləri yuxarı səviyyəli təsnifatçılar tərəfindən həlledici qaydanın formalaşmasında köməkçi olan aralıq nəticələr kimi nəzərdən keçirilir [3].

Nəticə. Bu işdə şəbəkə hücumlarının aşkarlanması və təsnifatı metodlarının müqayisəli təhlili aparılmışdır. Nəzərdən keçirilmiş yanaşmalar elmi ictimaiyyət tərəfindən hücumların aşkarlanması sistemlərinin hazırlanmasında uğurla istifadə olunur. Nəzərdən keçirilmiş yanaşmaların təsnifat sxemi təklif olunub. Şəbəkə anomaliyalarının aşkar edilməsi vəzifələrində məlumatların intellektual təhlili üsullarından istifadə təklifləri verilmişdir.

Kompüter təhlükəsizliyi laboratoriyasında son bir neçə il ərzində aktiv olaraq hücumların aşkarlanması sahəsində tədqiqatlar aparılır, o cümlədən çoxaqentli texnologiyaların istifadəsi sahəsində ikinci dərəcəli qurdların aşkar edilməsi üçün, şəbəkə qurdlarından qorunma mexanizmləri, zərərli faylların aşkar edilməsi.

Hazırda hücumların aşkarlanması sistemlərinin layihələndirilməsində perspektivli istiqamətlər siqnal və evristik metodların üstünlüklərini birləşdirməyə imkan verən yanaşmaların hibridləşdirilməsi, habelə böyük məlumat texnologiyalarından və proaktiv təhlükəsizlik monitorinqindən istifadə ediləcək. Bu qərarlara qarşı irəli sürülən yeni tələblərdən biri həqiqi və ya həqiqi miqyasda yaxın təhlükəsizlik məlumatlarının intellektual idarə edilməsini təmin edən hadisələrin adaptiv və yüksək miqyaslı analitik işlənməsini təmin etməkdir.

Ədəbiyyat

1.https://jpis.az/uploads/article/az/development_of_a_general__scheme_of_information_attacks_in_the_computer_network_based_on_the_classification_of_different_aspects___azerb._.pdf
2.Qasımov V.Ə. İnformasiyanın qorunmasının müasir texnologiyaları. Dərslik. Bakı. MTN-in Heydər Əliyev adına Akademiyasının nəşriyyatı. 2011, - 112 s.
3.http://www.spiiras.nw.ru/dissovet/wp-content/uploads/2018/06/branitskiy_dissertation.pdf
4.https://www.researchgate.net/publication/301610141_Analysis_and_Classification_of_Methods_for_Network_Attack_Detection
5.https://cyberleninka.ru/article/n/metody-obnaruzheniya-anomaliy-i-vtorzheniy
6.http://www.spiiras.nw.ru/dissovet/wp-content/uploads/2018/06/branitskiy_dissertation.pdf

CLASSIFICATION OF METHODS FOR DETECTING ATTACKS ON COMPUTER NETWORKS

dosent Mammadov Mahil Isa, Huseynova Dilkesh Bakhtiyar,
Aliyeva Ayten Natig, Mammadova Sima Kamaladdin

Summary

In modern times, the rapid development of information and communication technologies, especially computer networks, creates a number of problems related to the security of network resources that require new approaches. Currently, installing intrusion detection systems is a current issue in the field of network technologies. The article provides an analysis of the main methods for detecting and classifying network attacks and provides a generalized scheme for classifying these methods. The article discusses various methods of detecting network attacks. The main focus is to create a generalized classification scheme of network attack detection methods that presents the essence of each of the methods discussed and their comparative analysis within the proposed classification scheme.

КЛАССИФИКАЦИЯ МЕТОДОВ ОБНАРУЖЕНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ

Доцент Мамедов Махил Иса оглы, Гусейнова Дилкеш Бахтияр кызы,
Алиева Айтен Натиг кызы, Мамедова Сима Камаладдин кызы

Резюме

В наше время быстрое развитие информационных и коммуникационных технологий, особенно компьютерных сетей, создает ряд проблем, связанных с безопасностью сетевых ресурсов, которые требуют новых подходов. В настоящее время создание систем обнаружения атак является актуальной задачей в области сетевых технологий.

В статье представлен анализ основных методов обнаружения и классификации сетевых атак, а также предложена обобщенная схема классификации этих методов.

В статье рассматриваются различные методы обнаружения сетевых атак. Основное внимание уделяется созданию обобщенной схемы классификации методов обнаружения сетевых атак, отражающей суть каждого из рассмотренных методов и их сравнительный анализ в рамках предложенной схемы классификации.

Rəyçi: dos. Ağayev Vüqar
İnformasiya texnologiyaları kafedrasının 16 aprel 2021 –ci il tarixli 11 saylı iclas protokolu
Daxilm olma tarixi 19 aprel 2021-ci il