Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 15, брой 3, 2017 г.
Научно списание **http://www.mtc-aj.com** **статия № 1470**

СИСТЕМИ ЗА ДЕТЕКТИРАНЕ НА ИНТРУЗИЯ – ИЗПОЛЗВАНЕ НА ДОБРИТЕ ПРАКТИКИ ПРИ ОСИГУРЯВАНЕ НА ЗАЩИТАТА В АКАДЕМИЧНИ МРЕЖИ

Димитър Димитров[1], Антони Грънчаров[2]
ddimitrov@vtu.bg, office@pc4me.bg

[1]ВТУ "Тодор Каблешков", ул. Гео Милев 158, гр. София
[2]IT фирма PC4ME, ул. Александър. фон Хумболт 1, гр. София
БЪЛГАРИЯ

Ключови думи: *информационна сигурност, информационни системи, интернет, компютърни системи и мрежи, системи за детектиране на интрузия.*

Резюме: *Системите за детектиране на интрузия (прониквания) са предимно софтуерни инструменти, чрез които се следят компютърните системи и мрежи за злонамерени действия или нарушение на правилата за нормалната работа на мрежата. Всяка установена дейност или нарушение обикновено се анализира от администратора на мрежата, или се събира централно от система за управление на сигурността на събитията. Тези системи диагностицират трафика и чрез техниките си за филтриране алармират за злонамерената дейност, като се опитват също да ограничат истинските от фалшивите аларми.*

Университетските мрежи са особено уязвими на интрузия, както отвън, така и отвътре. Те могат да бъдат използвани за неправомерни действия, а контролът и управлението на мрежата в повечето случаи е ниско бюджетно. Всичко това прави тези въпроси особено актуални, а решението трябва да е адекватно и ефективно.

В настоящата статия се представя внедрената информационна система Snort и специфични особености на работа на академичната мрежа на ВТУ „Тодор Каблешков" за детектиране на интрузия, както и използваната система за управление на сигурността на информацията.

ВЪВЕДЕНИЕ

Въпросът за сигурността на информационните и комуникационни системи (ИКС) става все по-актуален напоследък и е свързан с комплексната реализация както на функционалността на самите системи, така и с осигуряване на достатъчно ниво на защита и интегритет на данните в тях. Определянето на нивото на сигурност на ИКС е свързано с оценката на възможните и вероятните атаки, на които те могат да бъдат подложени. Всяко неоторизирано и умишлено проникване в ИКС и/или промяната на информация в нея се нарича интрузия или атака. Интрузията може да доведе до редица материални и нематериални загуби, и да приведе системата от работоспособно в опасно състояние. В този случай само активното противодействие на интрузията може да възстанови отново нейното работно състояние, но вече в защитен режим и състояние на противодействие на атаката. [5, 6]

Сигурността на ИКС за осигуряване на защита срещу интрузия се свързва както със защитата на комуникационните ресурси на мрежата, така и със защитата на информацията, намираща се в нея. Основните елементи на защита на информацията се свързва с нейната конфиденциалност, интегритет (цялостност и непроменимост) на данните, надеждност на предаваната информация и автентификация на потребителите.

Оценката на мрежовата сигурност може да има преки финансови измерения, но когато се касае за специални организации (военни, антитерористични, изследователски и др.) принципът за икономически баланс не е водещ.

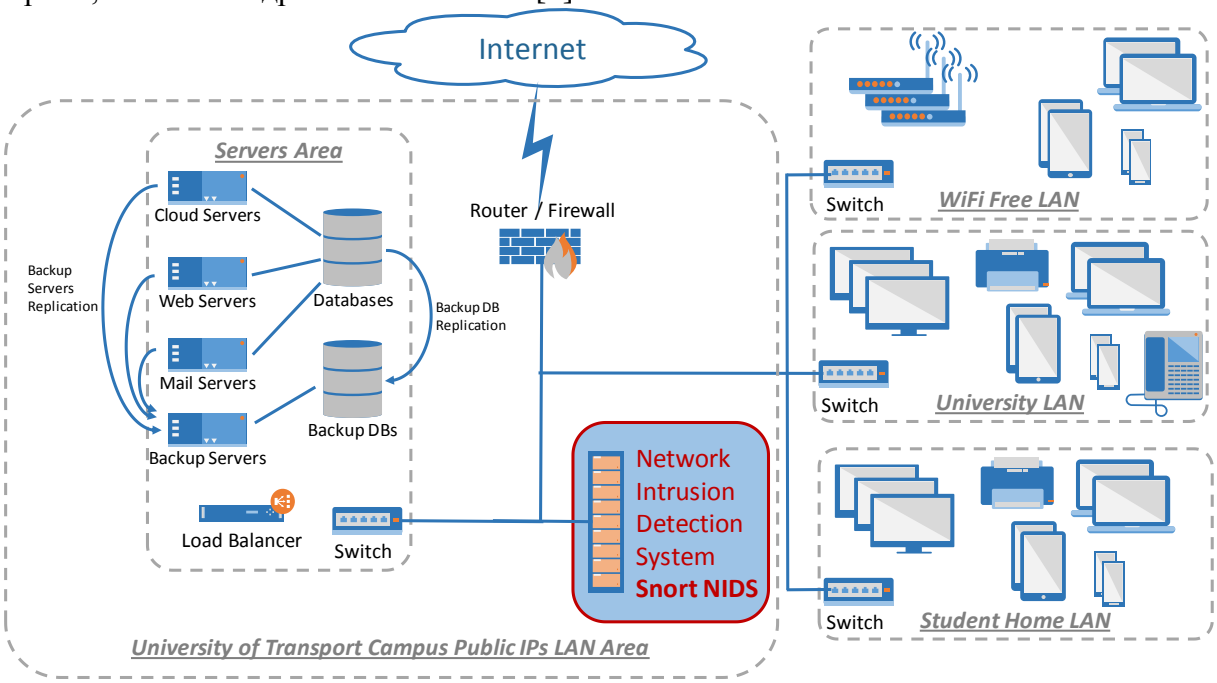
Университетските мрежи [1, 2, 3, 4] са особено уязвими на интрузия както отвън, така и отвътре. Те могат да бъдат използвани за неправомерни действия, а контролът и управлението на мрежата в повечето случаи е ниско бюджетно. Всичко това прави тези въпроси особено актуални, а решението трябва да е адекватно и ефективно.

В настоящата статия се представя внедрената информационна система SNORT и специфични особености на работа на академичната мрежа на ВТУ „Тодор Каблешков“ за детектиране на интрузия, както и система за управление на сигурността на информацията.

МОДЕЛ НА МРЕЖОВАТА СИСТЕМА ЗА ДЕТЕКТИРАНЕ НА ИНТРУЗИИ

Мрежово-базираните системи за детектиране на интрузия (Network-based Intrusion Detection Systems - NIDS) анализират мрежовия трафик (пакети) за наличие на определени поредици от символи (сигнатури) в тях. Мрежата може да е разделена на физически или логически сегменти и NDIS получава целия трафик от даден мрежов сегмент. NDIS анализират потока от данни, постъпили или напуснали сегмента или мрежата, анализира информационните събития за интрузионна активност и алармира ако открие такава. Обичайно това са информационни събития целящи единична или разпределена атака на IT ресурс или услуга, наличие на необичайна активност от определени източници на трафик (хостове или мрежи); аномалии в заглавните части (header) на комуникационните протоколи в анализираните пакети; необичайни събития в мрежата и др. [7, 8]

На фиг. 1 се показва общата схема на изградената университетска компютърна мрежа, както и внедрената Snort NIDS [9].



Фиг. 1. Обща схема на университетската компютърна мрежа и Snort NIDS.

Архитектурата на NIDS работи с пренасочения трафик от Router/Firewall и включва следните елементи:

-мрежов снифер;

-модул за предварителна обработка;

-модул за статистически анализ;

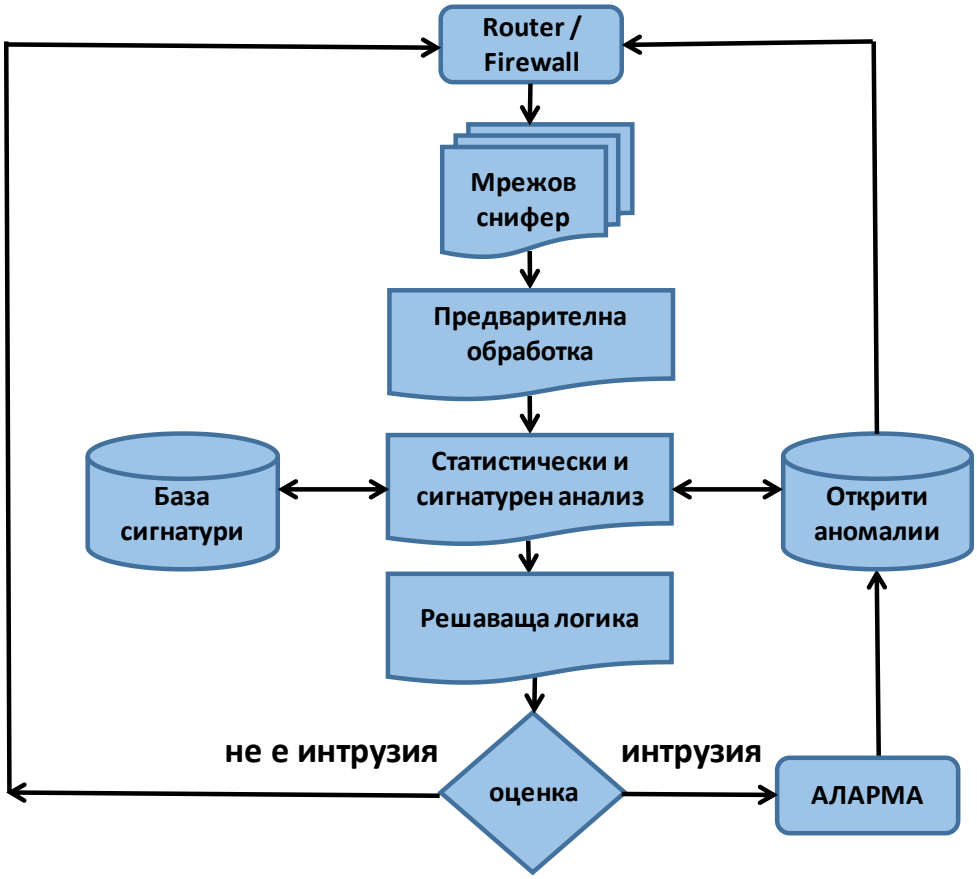
-модул за сигнатурен анализ;

-база данни с предварително дефинирани сигнатури;

-база данни с открити аномалии;

-решаваща логика, затова дали даден пакет или източник е интрузионен или не.

На фиг. 2 се показва алгоритъма за работа на логиката на NIDS в академичната мрежа.



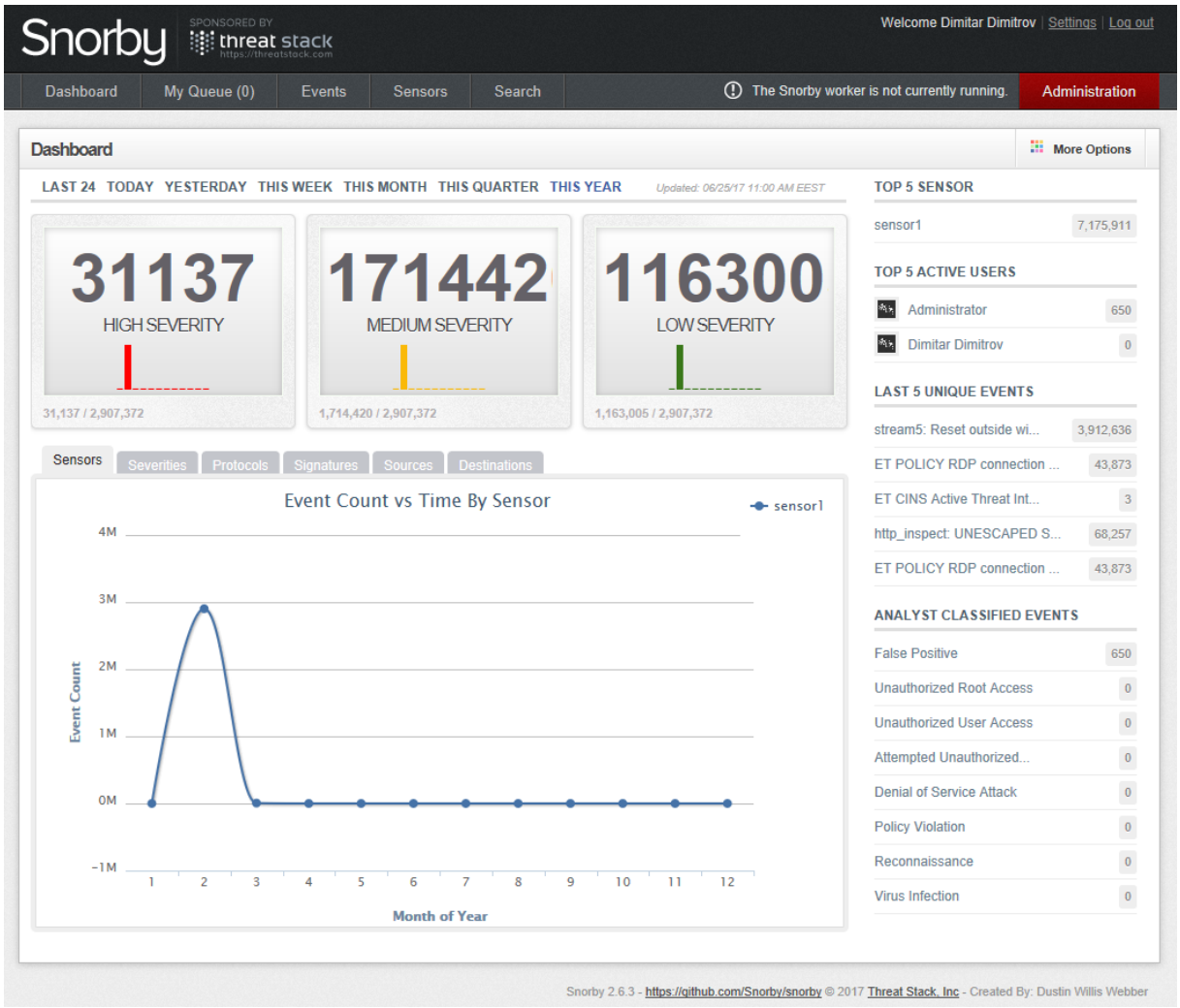
Фиг. 2. Алгоритъм за работа на NIDS.

Тук трябва да се отбележи, че системата може да премине и през т.нар. „процес на обучение“, в който се калибрира нейната работа и с оглед намаляване на фалшивите аларми. Системата позволява да се кодират и специфични правила за предпазване от интрузия, които управляват сигурността.

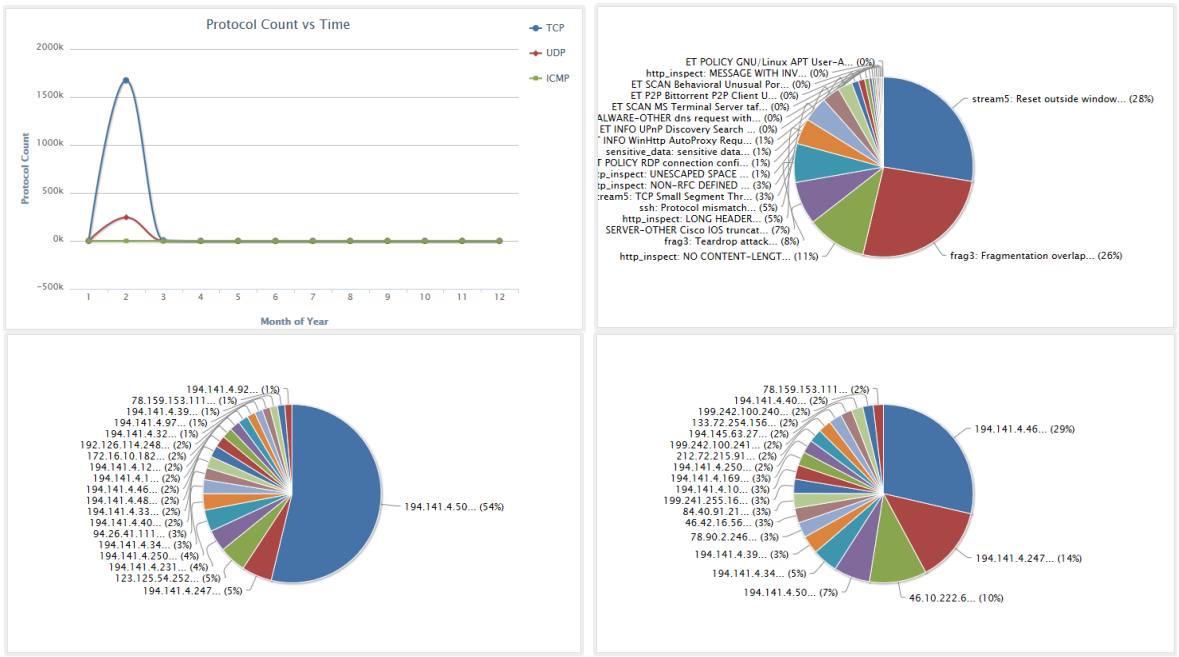
NIDS ФУНКЦИОНАЛНО РЕШЕНИЕ В АКАДЕМИЧНА МРЕЖА

Внедрената система Snort NIDS [9] е разгърната и адаптирана за академичната мрежа на ВТУ „Т. Каблешков“. Към настоящия момент тя се използва за анализ и натрупване на интрузионната активност в мрежата. Обвързана е с firewall системата и позволява да се прилагат нови правила за защита от външния трафик.

На следващите фигури се представят резултатите от работата на внедрената в университетската мрежа системата Snort NIDS. Входящият трафик по основните сегменти на мрежата се анализира и филтрира от NIDS, а визуализацията на резултатите се базира на графичния инструмент Snorby [10].



Фиг. 3. Общ изглед на основния визуализиращ екран на внедрената система NIDS.



Фиг. 4. Графики, показващи резултати от интрузионната активност в мрежата по протоколи на работа, сигнатури, адреси източници и адреси дестинации.

Системата Snorby има много добър инструментариум за визуализация на интрузионните проблеми в мрежата. Възможностите за сечения и детайлизация на справките позволява администраторите на мрежата да направят бърза и ефективна диагностика на проблемните сегменти точки. Това подпомага прилагането на ефективни мерки по филтриране на трафика и решаване на проблема с интрузията в мрежата.

ЗАКЛЮЧЕНИЕ

Настоящият доклад представи обобщен мрежов модел за детектиране на интрузия в академична мрежа. Въпросът е особено актуален и значим, тъй като те могат да бъдат използвани за неправомерни действия, а контролът и управлението на тези мрежи в повечето случаи е ниско бюджетно. Това прави въпроса много значим, а търсенето на решение на проблема изисква висока степен на автоматизация и работна стабилност.

Представя се още и внедрената система Snort с внедрените в нея добри практики за нейното използване, чрез които се осъществява регистрирането и анализът на интрузионните проблеми в мрежата. Внедрена е още и графичната система Sborby, чрез която се визуализират интрузионните активности в мрежата. Това е солидна основа за подобряване на информационната сигурност от заплахите в киберпространството.

ЛИТЕРАТУРА:

[1] Dimitrov D., Implementation of Contemporary Technologies in Virtualization and Construction of an Information Cloud of Systems for University Needs in the Field of Transport Education, , Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education – ICAICTSEE-2014, UNWE, Sofia, 2014.

[2] Dimitrov D., System for monitoring of the university computer network performance, , Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education – ICAICTSEE-2012, UNWE, Sofia, 2012.

[3] Димитров Д., Логическо развитие на мрежата в университетски кампус, , Сборник доклади на международна научна конференция "Приложение на информационните и комуникационни технологии в икономиката и образованието", ICAICTEE-2011, УНСС, София, 2011 г.

[4] Димитров Д., Проектиране и изграждане на автономна система за комплексно разпространение на интернет услуги в университетски кампус, , Научно списание „Механика Транспорт Комуникации”, ISSN 1312-3823, брой 3, 2011 г., статия № 0641, 2011 г.

[5] Христов Х., Трифонов В, Надеждност и сигурност на комуникациите, София, Нови знания, 2005 г.. ISBN 954-9315-43-6

[6] Hristov H., Trifonov. V., Security Of Telecommunication Networks: A Dominant Feature Within Current Safety Problems., International Journal on Information Technologies & Security N 2, 2009 p.19-27

[7] Trifonov. V., Model of Distribution Intrusion Detection System, International Journal on Information Technologies & Security N 2, 2010 p.67-73

[8] Trifonov. V., Nenova M., Theoretical Model of Distributed Intrusion Detection System Security and Safety, TELECOM’ 2010, 14-15 October, NSTC, Sofia, Bulgaria

[9] https://www.snort.org/
[10] https://github.com/Snorby/snorby

INTRUSION DETECTION SYSTEMS - USING THE GOOD PRACTICES IN PROVIDING PROTECTION IN ACADEMIC NETWORKS

Dimitar Dimitrov[1], Antony Grancharov[2]
ddimitrov@vtu.bg, office@pc4me.bg

[1]Todor Kableshkov University of Transport, 158 Geo Milev Str., Sofia,
[2]PC4ME IT Company, Alexander Street. Von Humboldt 1, Sofia
BULGARIA

Key words: *information security, information systems, internet, computer systems and networks, intrusion detection systems.*

Abstract: *Intrusion detection systems are mostly software tools that monitor computer systems and networks for malicious actions or violate rules for normal network operation. Any detected activity or violation is typically analyzed by the network administrator or centrally collected by an event security management system. These systems diagnose traffic and, through their filtering techniques, alert themselves to malicious activity, also trying to limit real from false alarms.*

University networks are particularly vulnerable to intrusion, both internally and externally. They can be used for malicious actions, and network control and management is in most cases low budget. All this makes these issues particularly relevant and the solution must be adequate and effective.

This article presents the implemented Snort information system and specific features of the academic network of Todor Kableshkov University of Transport for intrusion detection as well as the information security management system used.