Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри УІБ
д.т.н. доц. Ткачук Р.Л.
_____
“____” _____2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему Виявлення небезпечних входжень у комп'ютерну мережу за допомогою систем виявлення вторгнень та забезпечення захисту такої мережі

Виконав:
студент 4 курсу,
групи КБ-41, спеціальності 125
«Кібербезпека»
(шифр і назва спеціальності)
Боднар Остап
(прізвище, ім’я, по батькові)

Керівник Андрій Лагун
(прізвище та ініціали)

Рецензент Марія Рашкевич
(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Остап Боднар «Виявлення небезпечних входжень у комп'ютерну мережу за допомогою систем виявлення вторгнень та забезпечення захисту такої мережі». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 63 с., 17 рис., 31 джерело.

Об'єктом дослідження є IDPS - системи виявлення та запобігання вторгнень.

Мета роботи – дослідження та аналіз роботи систем виявлення та запобігання вторгнень, тобто IDPS-системи.

Методи дослідження – вивчення наукової літератури з теми дослідження, нормативно-правової бази, аналітичний і порівняльний методи, методи системного аналізу, індукції.

У першому розділі розглядаються загальні поняття про системи виявлення та запобігання вторгнень. В другому розділі розглядається вибір методів та критеріїв досліджень IDPS. У третьому розділі відбувається аналіз сучасних IDPS-систем. Досліджуються особливості роботи та демонструються інтерфейси систем.

IDS/IPS СИСТЕМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, SNORT, SURICATA

ABSTRACT

Ostap Bodnar "Detection of dangerous intrusions into a computer network using intrusion detection systems and ensuring the protection of such a network." Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 3 sections, 63 pages, 17 figures, 31 sources.

The object of the study is IDPS - intrusion detection and prevention systems.

The purpose of the work is to study and analyze the operation of intrusion detection and prevention systems, ie IDPS-systems.

Research methods - the study of scientific literature on the research topic, regulatory framework, analytical and comparative methods, methods of systems analysis, induction.

The first chapter discusses general concepts of intrusion detection and prevention systems. The second chapter discusses the selection of methods and criteria for IDPS research. The third chapter analyzes modern IDPS systems. Features of operation are investigated and system interfaces are demonstrated.

IDS/IPS SYSTEMS, INFORMATION SECURITY, SNORT, SURICATA

Зміст

ЗАГАЛЬНІ ВИСНОВКИ

В результаті проведеної роботи були проаналізовані характеристики, особливості роботи систем виявлення та запобіганю вторгнень.

Системи виявлення вторгнень та запобігання вторгнень проводять моніторинг подій, що відбуваються в комп'ютерній системі або мережі, і аналізують їх на наявність ознак можливих інцидентів, які є порушеннями або неминучими загрозами порушення політик комп'ютерної безпеки, політик допустимого використання або стандартних методів забезпечення безпеки та здійснюють спроби зупинки виявлених можливих інцидентів. Деякі організації використовують IDPS для інших цілей, таких як виявлення проблем з політиками безпеки, документування існуючих загроз і утримання окремих осіб від порушення політик безпеки. IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації.

IDPS не можуть забезпечити повністю точне виявлення; всі вони генерують false positivse (невірне визначення доброякісної активності як шкідливої) і false negativse (нездатність ідентифікувати шкідливу активність).

Вибір правильної системи з точки зору компанії залежить від ряду факторів:

- Необхідного рівня захисту мережі;
- Сфери діяльності компанії;
- Підготовки фахівців;
- Бюджету організації.

На прикладі сучасної системи виявлення вторгень Snort було досліджено, відстеження дій в мережі, спроби сканування портів та брутфорс SSH-сервісу. Було показано звіти всіх подій, які відбулись в системі.

Це дало чітке розуміння роботи та для чого потрібні IDPS для організацій. Системи виявлення вторгнення є потужним і гнучким інструментом виявлення мережевих атак. Використання їх доцільно, так як з кожним днем кількість загроз, а відповідно і атак, зростає.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балацька В.С., Шабатура М.М. Дослідження комп'ютерної мережі сканером вразливості Nessus. Вісник Львівського державного університету безпеки життєдіяльності. 2019. Вип. 20. С. 6-11.

2. Балацька В.С., Шабатура М.М. Сканери вразливості комп'ютерної мережі. Захист інформації в інформаційно-комунікаційних системах: матеріали III Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 р. / ЛДУ БЖД. Львів, 2019.С. 34-36

3. Безопасность сетей [Електронний ресурс] // Национальний Открытый Университет ИНТУИТ - 2018 — Режим доступу до ресурсу: https://www.intuit.ru/studies/courses/102/102/lecture/2995.

4. Безопасность сетей гарантируют системы предотвращения вторжения [Електронний ресурс] / Василий Томилин // cnews - 2007 — Режим доступу до ресурсу: http://www.cnews.ru/reviews/free/security2007/articles/networks.shtml.

5. В чем разница между Snort и Cisco FirePOWER? [Електронний ресурс] // Habr – 2015 – Режим доступу до ресурсу: https://habr.com/ru/company/cisco/blog/268207/.

6. Войтович В.С., Гриник Р.О. Дослідження надійності використання протоколу IPsec для створення VPN. Зб. тез доповідей Всеукраїнська науково-практична інтернет-конференція "Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку" (м. Черкаси, 13-19 березня 2017 р.). Черкаси, 2017. С. 66-68.

7. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція "Інформаційна безпека в сучасному суспільстві" (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.

8. День сурка. Осваиваем сетевую IDS/IPS Suricata [Електронний ресурс] // xakep.ru – 2015 - Режим доступу до ресурсу: https://xakep.ru/2015/06/28/suricata-ids-ips-197/.

9. Довганич М. О. Методи та засоби захисту персонального інформаційного простору в контексті мережевої розвідки / М. О. Довганич, В. І. Ящук // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С. 79-81).

10. Информационная безопасность на практике [Електронний ресурс] // Spy-Soft – 2016 - Режим доступу до ресурсу: http://www.spy-soft.net/snort/.

11. Классификация IDS [Електронний ресурс] / Ш.А. Акбарова, А.А. Ганиев // moluch.ru - 2017 — Режим доступу до ресурсу: https://moluch.ru/archive/149/41931/.

12. Лиса Н. К., Сікора Л. С., Ткачук Р. Л., Тупичак Л. Л., Таланчук Р. Р., Федина Б. І., Федевич О. Ю. Інформаційні та когнітивні технології оцінки ситуації в автоматизованих системах управління в умовах дії завад і факторів збою. Комп'ютерні технології друкарства : зб. наук. пр. Львів : УАД, 2021. Т. 45. № 1. С. 110–130.

13. Национальная библиотека им. Н.Э. Баумана Bauman National Library [Електронний ресурс]. // ru.bmst.wiki – 2016 — Режим досупу до ресурсу: https://ru.bmstu.wiki/IDS_(Intrusion_Detection_System).

14. Обнаружение сетевого вторжения с помощью Наблюдателя за сетями Azure и средств с открытым исходным кодом [Електронний ресурс] // Microsoft – 2021 - Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/azure/network-watcher/network-watcher-intrusion-detection-open-source-tools.

15. Основы системы обнаружения вторжений Snort. Часть 3 — Запись предупреждений о вторжениях в MySQL [Електронний ресурс] // Helpu Group – 2018 - Режим доступу до ресурсу: https://helpugroup.com/osnovy-sistemy-obnaruzheniya-vtorzhenij-snort-chast-3-zapis-preduprezhdenij-o-vtorzheniyah-v-mysql/.

16. Офіційний сайт фірми OSSEC [Електронний ресурс] // OSSEC HIDS — 2021 -Режим доступу до ресурсу: https://www.ossec.net/.

17. Офіційний сайт фірми Snort [Електронний ресурс] // Snort IDPS — 2021 - Режим доступу до ресурсу: https://www.snort.org/.

18. Офіційний сайт фірми Suricata [Електронний ресурс] // Suricata Open Source IDS / IPS / NSM engine — 2021 - Режим доступу до ресурсу: https://suricata-ids.org/.

19. Система обнаружения вторжений на базе IDS Snort [Електронний ресурс] // OpenNET – 2007 – Режим доступу до ресурсу: https://www.opennet.ru/base/sec/snort_ids.txt.html.

20. Системы и методы обнаружения вторжений: современное состояние и направление совершенствования [Електронний ресурс] / А.А. Корниенко, И.М. Слюсаренко // citforum.ru. - 2018 - Режим доступу до ресурсу: http://citforum.ru/security/internet/ids_overview/.

21. Системы обнаружения вторжений. Разворачиваем Snort и пишем правила [Електронний ресурс] // Эксплойт — 2018 - Режим доступу до ресурсу: https://telegra.ph/Sistemy-obnaruzheniya-vtorzhenij-Razvorachivaem-Snort-i-pishem-pravila-11-25.

22. Эффективный поиск на сайте с помощью Elasticsearch [Електронний ресурс] // codex – 2016 - Режим доступу до ресурсу: https://codex.so/elastic-search.

23. Ящук В. І. Кібернетична розвідка на основі методології та інструментарію OSINT / В.І. Ящук // Інформаційні технології в економіці, менеджменті та бізнесі. Проблеми науки, практики і освіти: Матеріали XXVI міжнарод. наук.-практ. Інтернет-конф., Київ, 26 листопада 2020 р. / Редкол.: І. І. Тимошенко та ін. – К. : Вид-во Європейського університету, 2020. – 270 с. (С.202-205).

24. Ящук В.І. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктури матеріали Міжнародної науково-практичної конференції “Сучасні напрями розвитку економіки, підприємництва, технологій та їх правового забезпечення” 02-03 червня 2021 року м. Львів

25. Create an OSSEC Log Management Console with Kibana [Електронний ресурс] // vichargrave – 2015 - Режим доступу до ресурсу: https://vichargrave.github.io/tutorials/create-an-ossec-log-management-console-with-kibana-4/.

26. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58

27. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58

28. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115

29. Scarfone K., Mell P. Guide Intrusion Detection and Prevention Systems (IDPS) / Karen Scarfone, Peter Mell – 2007

30. Suricata User Guide [Електронний ресурс] // Suricata – 2021 - Режим доступу до ресурсу: https://suricata.readthedocs.io/en/suricata-4.1.2/.

31. Tereykovsky I., Korchenko A., Parashchuk T., Pedchenko Y., Open intrusion detection systems analysis // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 3, c. 209-210