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 управління інформаційною безпекою, д. т. н., доцент
полковник служби цивільного захисту

_____ Ростислав ТКАЧУК
“____” _____2022 року

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: **«Дослідження технологій створення мережевих пасток для захисту комп’ютерних мереж»**

Виконав:
здобувач IV курсу, групи КБ-41
спеціальності (освітньої-професійної програми)
125 “Кібербезпека”
(Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої-професійної програми))
Анастасія СЕНИШ
(ім’я та прізвище)
Керівник Андрій ЛАГУН
(ім’я та прізвище)
Рецензент Марта МАШЕВСЬКА
(ім’я та прізвище)

Львів – 2022 року

АНОТАЦІЯ

Сениш Анастасія «Дослідження технологій створення мережевих пасток для захисту комп'ютерної мережі».

Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 60 с., 42 рис. Також – графічної (презентації) частини, що містить 12 слайдів.

Об'єкт – програми та методи для створення HoneyPot.

Предмет дослідження – особливості використання різних методів та програм на різних системах.

Мета дослідження - ознайомитись з історією створення даної технології, його класифікацією та видами, перевагами та недоліками, створити нову пастку HoneyPot з усіх можливих інструментів, правильно провести налаштування, також використати програму та перевірити як буде працювати і реагувати під час атаки на неіснуючу систему.

У даній бакалаврській кваліфікаційній роботі розглянуто питання про несанкціонований доступ в мережі, вибрано декілька методів і засобів захисту від зловмисників, описано вибрані програми для подальшої реалізації, реалізована робота HoneyPot на віртуальній машині/на ОС Windows/на Android, проведено аналіз змін стану системи до/під час/після роботи пастки та підведено підсумки.

КОМП'ЮТЕРНА МЕРЕЖА, МЕРЕЖЕВА ПАСТКА, ЗАСОБИ ЗАХИСТУ, МЕТОДИ ЗАХИСТУ, ІНСТРУМЕНТИ, НАЛАШТУВАННЯ, ВІРТУАЛЬНА МАШИНА, СИСТЕМА, WINDOWS, ANDROID.

ABSTRACT

Senysh Anastasia «Technology research of network traps for protection of a computer network».

Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 3 sections, 60 pages, 42 figures. Also – a graphic (presentation) part containing 12 slides.

Object – programs and methods for creating a HoneyPot.

The subject for research – features of using different methods and programs on different systems.

The purpose of the work is to get acquainted with history of creation this technology, its classification and types, advantages and disadvantages, creating a new trap HoneyPot from all possible tools, make the correct settings, also use the program and test how it will work and its reaction during the attack on a non-existing system.

This thesis considers the unauthorized access to the network, chosen a few methods and funds of protection, described chosen programs for future realization, realized work of HoneyPot on virtual machine/ on OS Windows/ on Android-system, analyzed changes of system condition before/during/after working traps and made a conclusion.

COMPUTER NETWORK, NETWORK TRAP, FUNDS OF PROTECTION, METHODS OF PROTECTION, TOOLS, SETTINGS, VIRTUAL MACHINE, SYSTEM, OS WINDOWS, ANDROID-SYSTEM.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

В даній бакалаврській кваліфікаційній роботі було проведено такі дослідження:

- вивчено історію походження HoneyPot та його класифіковано на декілька видів;
- ознайомлено з інструментів різних типів та рівнів взаємодії, наведено приклади програм;
- вибрано основні, на теперішній час, інструменти, які можуть допомогти у реалізації HoneyPot;
- створено власну «пастку» для розслідування зловмисних дій;
- правильно налаштовано HoneyPot для правильної роботи;
- перевірка поведінки HoneyPot та стану системи після атаки;
- підведені підсумки та вибрано найкращі методи для створення пастки і подальшої роботи з нею.

Завдяки пунктам, які наведені вище, була досягнута успішна реалізація у створенні та налаштуванні власного HoneyPot та проведена робота з перевіркою на працездатність «пастки».

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. А.Кичма, О.Полотай Загрози безпеки Wi-Fi мереж та основні протоколи захисту. "Інформаційна безпека та інформаційні технології": Збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів учених, студентів і курсантів. – Львів, 2021. – С. 49-51.

2. 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.

3. Войтович В.С., Мандрона М.М. Класифікація Honeypot технологій та тип взаємодії для захисту комп'ютерної мережі. Зб. наук. праць XIII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів "Проблеми та перспективи розвитку системи безпеки життєдіяльності" (м. Львів, 22-23 березня 2018 р.). Львів: ЛДУ БЖД, 2018. С. 214–215.

4. Войтович В.С., Мандрона М.М. Технологія Honeypot для захисту комп'ютерної мережі. Збірник тез доповідей III Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології" (м. Кропиницький, 19-20 квітня 2018 р.). Кропивницький: ЦНТУ, 2018. С. 45–46.

5. Войтович В.С., Шабатура М.М. Принцип дії технології Honeypot для захисту комп'ютерної мережі. Зб. тез доповідей III Міжвузівської науково-практичної конференції студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах" (м. Львів, 29-30 листопада 2018 р.). Львів: ЛДУ БЖД, 2018. С. 72–74.

6. 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).

7. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю. Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

8. Кленик О., Ткачук Р. Особливості побудови захищеної мережі підприємства. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології" (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 52–54.

9. Колядич І., Ткачук Р. Системи автоматичного керування програмним забезпеченням. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів "Інформаційна безпека та інформаційні технології" (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 55–57.

10. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

11. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції "Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України" (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 84–85.

12. Ориник С. Забезпечення безпеки використання хмарних сховищ для захисту персональних даних / С. Ориник, В. Ящук // Інформаційна безпека та

інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

13. Шахуб С. М., Ткачук Р. Л. Дослідження методів і засобів при запроваджені концепції BYOD на підприємстві. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції "Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України" (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 149–150.

14. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

15. Comprehensive Guide on Honeypots [Електронний ресурс] Режим доступу до ресурсу - https://www.hackingarticles.in/comprehensive-guide-on-honeypots/

16. History of HoneyPots [Електронний ресурс] Режим доступу до ресурсу - https://flylib.com/books/en/1.48.1.14/1/

17. Honeypot (computing) [Електронний ресурс] Режим доступу до ресурсу - https://www.techtarget.com/searchsecurity/definition/honey-pot

18. HoneyPots [Електронний ресурс] Режим доступу до ресурсу - http://www.123seminarsonly.com/Seminar-Reports/012/53599210-Honey-Pots.pdf

19. HoneyPots: Are they Illegal [Електронний ресурс] Режим доступу до ресурсу - https://web.archive.org/web/20080515205741/http://www.securityfocus.com/infocus/1703

20. Honeypots: Tracking Hackers [Електронний ресурс] Режим доступу до ресурсу - https://web.archive.org/web/20090401184953/http://www.tracking-hackers.com/

21. HosTaGe [Електронний ресурс] Режим доступу до ресурсу - https://www.informatik.tu-

darmstadt.de/telekooperation/research_2/smart_protection_in_infrastructures_and_networks_spin/showcases/hostage/index.en.jsp

22. Nmap tutorial: how to use nmap and ZenMap [Електронний ресурс] Режим доступу до ресурсу - https://www.ictshore.com/hacking/nmap-tutorial/

23. 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.

24. 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.

25. 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.

26. PenTBox [Електронний ресурс] Режим доступу до ресурсу - https://pentestlab.blog/2013/02/03/pentbox/

27. Pentbox Honeypot [Електронний ресурс] Режим доступу до ресурсу - https://www.sevenlayers.com/index.php/255-pentbox-honeypot

28. Pentbox is a simple honeypot for beginners [Електронний ресурс] Режим доступу до ресурсу - https://schoolchore.com/2022/04/22/pentbox-is-a-simple-honeypot-for-beginners-to-use-honeypots-can-give-you-a-good/

29. Pentbox/README.md [Електронний ресурс] Режим доступу до ресурсу - https://github.com/technicaldada/pentbox/blob/master/README.md

30. Trap for Hacker!!! HoneyPot | How to Set up HoneyPot [Електронний ресурс] – Режим доступу до ресурсу - https://hackingblogs.com/setup-honeypot/

31. Wat is een honeypot [Електронний ресурс] Режим доступу до ресурсу - https://www.kaspersky.nl/resource-center/threats/what-is-a-honeypot