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 **Розробка методології аналізу вразливостей та тестування засобів захисту веб-серверів у віртуальній лабораторії**

Виконав:
здобувач IV курсу, групи КБ-41
спеціальності (освітньої-професійної програми)
125 “Кібербезпека”
(Управління інформаційною безпекою)
(шифр і назва спеціальності (освітньої-професійної програми))
Дарія ГОНЧАРОВА
(ім’я та прізвище)
Керівник Тарас БРИЧ
(ім’я та прізвище)
Рецензент Марія ШАБАТУРА
(ім’я та прізвище)

Львів – 2022 року

АНОТАЦІЯ

Дарія Гончарова “Розробка методології аналізу вразливостей та тестування засобів захисту веб-серверів у віртуальній лабораторії”. Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 63 сторінки, 41 рисунок, 30 джерел.

Об'єктом дослідження є інформаційна безпека веб-серверів.

Мета роботи: розробка віртуальної лабораторії для тестування безпеки веб-серверів, проведення аналізу вразливостей та визначення можливих методів їх усунення.

Предмет дослідження: методи та засоби тестування серверів на вразливості.

Методи дослідження: вивчення відкритих джерел на тему дослідження, нормативно-правової бази, аналітичний і порівняльний методи, розробка програмних продуктів, методи системного аналізу.

Практична значущість: полягає у створені віртуальної лабораторії з використанням free software з можливістю швидкого розгортання для тестування веб-серверів перед підключенням їх до Інтернету.

ІНФОРМАЦІЙНА БЕЗПЕКА, ВІРТУАЛЬНІ ТЕСТОВІ ЛАБОРАТОРІЇ, ВЕБ-СЕРВЕРИ, VIRTUALBOX, APCHE, NGINX, METASPLOIT.

ABSTRACT

Dariia Honcharova “Development of a methodology for vulnerability analysis and web server security testing in a virtual laboratory”. Graduation work on the specialty 125 “Cybersecurity” consists of a text part containing 3 sections, 63 pages, 41 figures, 30 sources.

The object of study is information security of web servers.

The goal is to: development of a virtual laboratory for testing the security of web servers, analyzing vulnerabilities and identifying possible methods for resolving them.

Subject of research: methods and tools for testing servers for vulnerabilities.

Research methods: study of open sources on the topic of research, regulatory framework, analytical and comparative methods, software development, methods of systems analysis.

Practical significance: is to create a virtual lab using free software with the ability to quickly deploy to test web servers before connecting them to the Internet.

INFORMATION SECURITY, VIRTUAL TEST LABORATORIES, WEB SERVERS, VIRTUALBOX, APCHE, NGINX, METASPLOIT.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

В даній дипломній роботі було проведено аналіз вразливостей та загрози безпеки веб-серверів. Особлива увага приділялась методам та інструментам тестування захисту веб-серверів, характеристиці знайдених вразливостей, а також способам їх усунення. Було розглянуто принцип роботи віртуальних машин та проведено тестування безпеки веб-серверів Apache та Nginx, встановлених на гіпервізорі VirtualBox, з хостової системи Ubuntu 20.04 і гостьової – Kali Linux.

Метою роботи було створення віртуальної лабораторії для тестування безпеки веб-серверів, проведення аналізу знайдених вразливостей та визначення можливих способів та засобів їх усунення. Поставлена мета досягнута у повному обсязі. Для цього було виконано такі завдання:

- розглянуто поняття веб-серверів та механізм їх роботи;
- проаналізовано різницю між вразливостями та загрозами;
- розглянуто поширені атаки на веб-сервери та їх наслідки;
- розглянуто поняття аналізу та тестування вразливостей;
- проведено аналіз відмінностей віртуалізації та контейнеризації;
- створено віртуальну лабораторію за допомогою інструментів автоматизованого створення та налаштування віртуальних машин;
- проведено сканування вразливостей веб-серверів Apache та Nginx;
- визначено можливі способи усунення вразливостей;

- проведено тестування на проникнення за допомогою Metasploit.

Необхідно постійно проводити тестування вразливостей різноманітними інструментами та впроваджувати захист веб-серверів, оскільки нехтування політики безпеки може призвести до втрати конфіденційних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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. 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.

4. Балацька В.С., Ящук В.І., Полотай О.І. Вразливість комп'ютерної мережі як проблема закладів вищої освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи: збірник тез доповідей VI Міжнародній науково-практичній конференції (м. Київ - м. Львів, 4-5 листопада 2021 р.). Львів: ЛДУ БЖД, 2021. С. 66–68.

5. Вербицький С.Т., Брич Т.Б, Купльовський Б.Є., Олещук Є.І., Прокопишин В.І., Прокопишин В.І., Вербицька О.С., Стецьків О.Т. Звіт НДР №: III-17-20, «Використання хмарних середовищ для обробки, зберігання та захисту даних сейсмологічних спостережень».

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. 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.

13. 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 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).

14. Ansible Community Documentation [Електронний ресурс]. Режим доступу: https://docs.ansible.com/ansible_community.html

15. Apache HTTP Server Documentation [Електронний ресурс]. Режим доступу: https://devdocs.io/apache_http_server/

16. 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.

17. HashiCorp Vagrant Documentation [Електронний ресурс]. Режим доступу: https://www.vagrantup.com/docs

18. How to Hack a Web Server? [Електронний ресурс]. Режим доступу: https://www.knowledgehut.com/blog/security/hacking-web-server

19. How To: Run Your First Vulnerability Scan with Nessus [Електронний ресурс]. Режим доступу: https://www.tenable.com/blog/how-to-run-your-first-vulnerability-scan-with-nessus

20. Kali Tools [Електронний ресурс]. Режим доступу: https://www.kali.org/tools/

21. Metasploit-Framework [Електронний ресурс]. Режим доступу: https://www.kali.org/tools/metasploit-framework/

22. Nginx Docs Product Documentation [Електронний ресурс]. Режим доступу: https://docs.nginx.com/

23. Nikto [Електронний ресурс]. Режим доступу: https://www.kali.org/tools/nikto/

24. 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.

25. 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.

26. 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.

27. OWASP ZAP Documentation [Електронний ресурс]. Режим доступу: https://www.zaproxy.org/docs/

28. Ultimate Guide to Server Security Vulnerabilities (And how to protect yourself!) [Електронний ресурс]. Режим доступу: https://www.eurovps.com/blog/server-security-vulnerabilities/

29. VirtualBox Documentation [Електронний ресурс]. Режим доступу: https://www.virtualbox.org/wiki/Documentation

30. VMWare Workstation Documentation [Електронний ресурс]. Режим доступу: https://docs.vmware.com/en/VMware-Workstation-Pro/index.html