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 Моделювання мережевих атак для тестування засобів захисту інформації

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

Керівник Володимир САМОТИЙ
(прізвище та ініціали)

Рецензент Богдан МІЗЮК
(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Ростислав Драбовський «Моделювання мережевих атак для тестування засобів захисту інформації». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 60 с., 13 рис., 1 таблицю, 61 джерела, 1 додаток.

Об'єктом дослідження є методика тестування на проникнення веб-серверів.

Мета роботи – підвищення ефективності та швидкості тестування на проникнення веб-серверів, методи порівняння.

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

У практичній частині розроблено методику тестування на проникнення. Розроблена методика враховує переваги існуючих методик тестування на проникнення у світі та містить перелік та опис інструментів для тестування.

У роботі також є аналіз поширених вразливстей у веб серверах, способи захисту від них, та оцінка вразливостей з використанням метрики CVSS.

Практичне значення роботи полягає у зниженні тривалості та обгрунтуванні вибору засобів та інструментів тестування на проникнення.

Результати здійснених у дипломній роботі досліджень можуть бути використані при тестуванні на проникнення веб-серверів.

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, ВЕБ-СЕРВЕР, ВРАЗЛИВІСТЬ, МЕТОДИКА, АТАКИ, ВЕБ-ДОДАТОК

ABSTRACT

Rostyslav Drabovskyj "Simulation of network attacks for testing information security tools". Thesis in the specialty of 125 "Cybersecurity" consists of textual part that contains 3 sections, 60 pages, 13 figures, 1 table, 61 sources, 1 addition.

The object of the study is a method of testing the penetration of web servers.

The purpose of the work is to increase the efficiency and speed of testing for web server penetration, comparison methods.

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

In the practical part the technique of penetration testing is developed. The developed methodology takes into account the advantages of existing methods of testing for penetration into the world and contains a list and description of tools for testing.

There is also an analysis of common vulnerabilities in web servers, ways to protect against them, and vulnerability assessment using CVSS metrics.

The practical significance of the work is to reduce the duration and justify the choice of means and tools for penetration testing.

The results of research conducted in the thesis can be used in testing the penetration of web servers.

PENETRATION TESTING, WEB SERVER, VULNERABILITY, METHODOLOGY, ATTACKS, WEB APPLICATION

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

У дипломній роботі була розроблена методика для можливості підвищення ефективності та швидкості тестування на проникнення. Для того, щоб досягти мети роботи, ми провели аналіз функціонування та стану веб-серверів. Також ми визначили та проаналізували поширенні вразливості веб-серверів, та можливості атак через вразливості, тому що важливим етапом тестування на проникнення є пошук вразливостей. Структури, які шукають уразливості, також були проаналізовані. Згідно з дослідженнями, ми знайшли стандарти обробки даних про уразливість, метрики критичності вразливостей та інструменти для їх пошуку. Проаналізували існуючи методики у світі. Та зробили висновок, що більшість методів охоплюють широкий спектр проблем кібербезпеки, тому необхідний додатковий час, що витрачається на аналіз вразливостей відповідно до існуючих методами і вибір, зокрема, тих компонентів, які підходять для тестування веб-додатків.

За допомогою результатів аналізу та досліження було розроблено адаптована методика, яка проникає в мережу, та враховує міжнародні досягнення в цьому напрямку. Саме тому дозволяє перевіряти наявність найбільш поширених вразливостей. А завдяки відбору тестування лише вразливостей лише з критичним рівнем ризику підвищується ефективність. Практична цінність роботи полягає в скороченні тривалості і обґрунтуванні вибору інструментів тестування на проникнення. Результат дипломної роботи може бути використаний для тестування на проникнення веб-додатків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alyshov O. bWAPP Веб безопасность [Електронний ресурс] / Orkhan Alyshov – Режим доступу до ресурсу: https://orkhanalyshov.com/blog/42.

2. Authentication Hacking: What are Authentication Hacking Attacks? [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.acunetix.com/websitesecurity/authentication/.

3. Blazquez D. Broken Authentication OWASP Top 10 - A2 [Електронний ресурс] / Daniel Blazquez. – 2019. – Режим доступу до ресурсу: https://hdivsecurity.com/owasp-broken-authentication.

4. Blazquez D. Sensitive Data Exposure OWASP Top 10 - A3 [Електронний ресурс] / Daniel Blazquez – Режим доступу до ресурсу: https://hdivsecurity.com/owasp-sensitive-data-exposure.

5. Brewer J. Web Server Vulnerabilities and a Defense in Depth Strategy Using the Squid Proxy [Електронний ресурс] / Jim Brewer // GSEC Practical version 1.4b. – 2004. – Режим доступу до ресурсу: https://www.giac.org/paper/gsec/3729/web-server-vulnerabilities-defense-in-depth-strategy-squid-proxy/105970.

6. Broken Authentication and Session Management [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://www.owasp.org/index.php/Broken_Authentication_and_Session_Management.

7. Charan H. Broken Authentication and Session Management [Електронний ресурс] / Hari Charan // DZone. – 2017. – Режим доступу до ресурсу: https://dzone.com/articles/broken-authentication-and-session-management-part.

8. Charan H. Broken Authentication and Session Management—part I [Електронний ресурс] / Hari Charan. – 2017. – Режим доступу до ресурсу: https://medium.com/@grep_security/broken-authentication-and-session-management-part-i-50e760c9f599.

9. Choudhary A. SQL Injection Attacks: Know How to Prevent Them [Електронний ресурс] / Archana Choudhary // Security Zone. – 2019. – Режим доступу до ресурсу: https://dzone.com/articles/sql-injection-attacks-know-how-to-prevent-them.

10. Cloudi. APT SIMULATOR [Електронний ресурс] / Cloudi. – 2018. – Режим доступу до ресурсу: https://hydrasky.com/network-security/kali-tools/apt-simulator/.

11. Cobb M. Cross-site scripting explained: How to prevent XSS attacks [Електронний ресурс] / Michael Cobb // 2009 – Режим доступу до ресурсу: https://www.computerweekly.com/tip/Cross-site-scripting-explained-How-to-prevent-XSS-attacks.

12. Common Vulnerability Scoring System Calculator Version 3 [Електронний ресурс] – Режим доступу до ресурсу: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

13. Common Vulnerability Scoring System v3.0 [Електронний ресурс] – Режим доступу до ресурсу: https://www.first.org/cvss/cvss-v30-specification-v1.7.pdf.

14. Common Vulnerability Scoring System v3.0: Specification Document [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.first.org/cvss/specification-document.

15. Common Vulnerability Scoring System v3.0: Specification Document [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.first.org/cvss/specification-document.

16. Common Website Security Vulnerabilities [Електронний ресурс] // Common places. – 2019. – Режим доступу до ресурсу: https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/.

17. Cross Site Scripting (XSS) Attack Tutorial With Examples, Types & Prevention [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/.

18. Cross Site Scripting (XSS) Attack Tutorial With Examples, Types &

Prevention [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/.

19. Cross-Site Request Forgery (CSRF) [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF).

20. Cross-site Scripting (XSS) [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS).

21. Excess XSS [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://excess-xss.com.

22. Ganore P. What Is A Web Server And How Does It Function? [Електронний ресурс] / Pravin Ganore. – 2017. – Режим доступу до ресурсу: https://www.milesweb.com/blog/hosting/web-server-function/.

23. How a Web server functions? [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: https://www.eukhost.com/blog/webhosting/how-a-web-server-functions/.

24. How to Prevent SQL Injection Attacks [Електронний ресурс] // eSecurityPlanet. – 2018. – Режим доступу до ресурсу: https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks.html.

25. How to Protect Against SQL Injection Attacks [Електронний ресурс] // UC Berkeley. – 2019. – Режим доступу до ресурсу: https://security.berkeley.edu/education-awareness/best-practices-how-articles/system- application-security/how-protect-against-sql.

26. Luka S. Обзор площадки для тестирования веб-уязвимостей OWASP Top-10 на примере bWAPP [Електронний ресурс] / Safronov Luka. – 2015. – Режим доступу до ресурсу: https://habr.com/ru/post/250551/.

27. Melnick J. Top 10 Most Common Types of Cyber Attacks [Електронний ресурс] / Jeff Melnick. – 2018. – Режим доступу до ресурсу: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

28. Nessus professional benefits [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.tenable.com/products/nessus/nessus-professional.

29. 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 1.

30. 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.

31. 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.

32. Ricca F. https://dl.acm.org/citation.cfm?id=381476 [Електронний ресурс] / F. Ricca, P. Tonella. – 2001. – Режим доступу до ресурсу: https://dl.acm.org/citation.cfm?id=381476

33. Safonov L. APTSimulator — тестирование противодействия APT угрозам [Електронний ресурс] / Luka Safonov. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/post/350066/.

34. Sankar R. Burpsuite – A Beginner’s Guide For Web Application Security or Penetration Testing [Електронний ресурс] / Ravi Sankar. – 2018. – Режим доступу до ресурсу: https://kalilinuxtutorials.com/burpsuite/.

35. Security Misconfiguration [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://bounty.github.com/classifications/security-misconfiguration.html.

36. Security Testing - Sensitive Data Exposure [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.tutorialspoint.com/security_testing/testing_sensitive_data_exposure.htm .

37. Singh S. 5 Practical Scenarios for XSS Attacks [Електронний ресурс] / Satyam Singh // Pentest Tools. – 2018. – Режим доступу до ресурсу:

https://pentest-tools.com/blog/xss-attacks-practical-scenarios/.

38. SQL инъекции. Проверка, взлом, защита [Електронний ресурс] // BVN2. – 2011. – Режим доступу до ресурсу: https://habr.com/ru/post/130826/.

39. SQL_Injection_Prevention_Cheat_Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SQL_Injection

40. TAMMANY J. https://www.sitelock.com/blog/owasp-top-10-sensitive-data-exposure/ [Електронний ресурс] / JOYCE TAMMANY // CYBER ATTACKS. – 2018. – Режим доступу до ресурсу: https://www.sitelock.com/blog/owasp-top-10-sensitive-data-exposure/.

41. Testing for CSRF (OTG-SESS-005) [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.owasp.org/index.php/Testing_for_CSRF_(OTG-SESS-005).

42. Testing for CSRF (OTG-SESS-005) [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.owasp.org/index.php/Testing_for_CSRF_(OTG-SESS-005).

43. Top 10-2017 A6-Security Misconfiguration [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.owasp.org/index.php/Top_10-2017_A6-Security_Misconfiguration.

44. Top 8 Network Attacks by Type in 2017 [Електронний ресурс] // CALYPTIX. – 2017. – Режим доступу до ресурсу: https://www.calyptix.com/top-threats/top-8-network-attacks-type-2017/.

45. Using Burp Proxy [Електронний ресурс] // 2018 – Режим доступу до ресурсу: https://support.portswigger.net/customer/portal/articles/1783119-using-burp-proxy.

46. Using Burp to Test for Sensitive Data Exposure Issues [Електронний ресурс] // PortSwigger. – 2018. – Режим доступу до ресурсу: https://support.portswigger.net/customer/portal/articles/1965730-using-burp-to-test-for-sensitive-data-exposure-issues.

47. Web Application Risk – the Threat of and Solution to Sensitive Data Exposure [Електронний ресурс] – Режим доступу до ресурсу: https://www.immuniweb.com/blog/OWASP-sensitive-data-exposure.html.

48. Web Server and its Types of Attacks [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://www.greycampus.com/opencampus/ethical-hacking/web-server-and-its-types-of-attacks.

49. Web Server Vulnerabilities Attacks: How to Protect Your Organization [Електронний ресурс] // Tech Funnel. – 2018. – Режим доступу до ресурсу: https://www.techfunnel.com/information-technology/web-server-vulnerabilities-attacks-how-to-protect-your-organization/.

50. Zeeshan N. 7 Ways To Stop Web Attacks Affecting Your Web Application [Електронний ресурс] / Nasrumminallah Zeeshan. – 2017. – Режим доступу до ресурсу: https://www.peerlyst.com/posts/7-ways-to-stop-web-attacks-affecting-your-web-application-nasrumminallah-zeeshan.

51. 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.

52. 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.

53. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // 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.121-124).

54. 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.

55. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів "Проблеми та перспективи розвитку системи безпеки життєдіяльності" (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.

56. 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.

57. Евтеев Д. SQL Injection от А до Я [Електронний ресурс] / Дмитрий Евтеев. – 2008. – Режим доступу до ресурсу: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-devteev-Advanced-SQL-Injection.pdf.

58. Инструменты Kali Linux [Електронний ресурс] – Режим доступу до ресурсу: https://kali.tools.

59. Методы защиты от CSRF-атаки [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://habr.com/ru/post/318748/.

60. Уязвимости веб-приложений [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Vulnerabilities-2019-rus.pdf.

Что такое веб-сервер [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://developer.mozilla.org/ru/docs/Learn/%D0%A7%D1%82%D0%BE_%D1%82%D0%B0%D0%BA%D0%BE%D0%B5_%D0%B2%D0%B5%D0%B1_%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80.

61. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня

2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).