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

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

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему Оптимізація використання програмного забезпечення grapheneX у зв'язці з Ansible для посилення безпеки ОС хостів у локальній мережі

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

Керівник БРИЧ Т.Б.
(прізвище та ініціали)

Рецензент КУПЛЬОВСЬКИЙ Б.Є
(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Богдан Пахомов «Оптимізація використання програмного забезпечення grapheneX у зв'язці з Ansible для посилення безпеки ОС хостів у локальній мережі». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 4 розділи, 53 сторінки, 2 рисунки, 43 джерел.

Об'єктом дослідження є інформаційна безпека хостів у локальній мережі автоматизація, посилення безпеки, ansible, grapheneX.

Мета роботи: розробити автоматизацію налаштовування хостів для посилення їх безпеки з використанням grapheneX у зв'язці з Ansible. Провести тестування розробленого продукту на створеному віртуальному середовищі. Розробити рекомендації для укріплення безпеки хостів у локальних мережах.

Предмет дослідження: автоматизація налаштувань безпеки комп'ютерів.

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 модифікації відкритого програмного забезпечення grapheneX, створенні модулів для нього та його автоматизації за допомогою ansible.

ANSIBLE, HARDENING, GRAPHENEX, АВТОМАТИЗАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВІРТУАЛЬНІ ТЕСТОВІ ЛАБОРАТОРІЇ.

ABSTRACT

Bohdan Pakhomov "Optimizing the use of grapheneX software in conjunction with Ansible to enhance the security of the host OS on the local network." Thesis on the specialty 125 "Cybersecurity" consists of a text part containing 4 sections, 53 pages, 2 figures, 43 sources.

The object of study is the information security of hosts in the local network automation, security enhancement, Ansible, grapheneX.

The goal is to: develop automation for setting up hosts to increase their security using grapheneX in conjunction with Ansible. Conduct testing of the developed product on the created virtual environment. Develop guidelines for strengthening the security of hosts on local networks.

Subject of research: automation of computer security settings.

Research methods: the 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 modify the open source software grapheneX, create modules for it and automate it with Ansible.

ЗМІСТ

ЗАГАЛЬНІ ВИСНОВКИ

Завдяки автоматизації безпеки команди інформаційної безпеки тепер оснащені рішенням, яке може працювати на них і виконувати всі завдання безпеки, що вимагало часу у фахівців з безпеки. Цінний час, який можна використати для залучення до більш стратегічної діяльності та роботи над активними заходами безпеки.

Є кілька ознак, які говорять про те, що завдання безпеки має бути автоматизованим:

- Повторювані повсякденні завдання
- Виснажливі, одноманітні завдання
- Завдання, що забирають багато часу

Ручна робота завжди передбачає, щонайменше, невелику можливість помилки людини та неточних даних. Використовуючи автоматизацію та усуваючи участь людини принаймні в одній області, можна значно зменшити ймовірність помилок, оскільки кожного разу дотримуються однакові правила та процедури. Крім того, впровадження в процес рішення автоматизації безпеки значно покращить точність і послідовність розслідувань та запобігання загроз, оскільки нудні завдання, де можуть виникати помилки, робляться за вас.

Усі вищезазначені переваги зводяться до цієї останньої, і часто цитованої, переваги автоматизації безпеки - поліпшення рентабельності інвестицій в автоматизацію та наявні засоби й рішення безпеки.

У першому розділі було розглянуто вже наявні засоби для автоматизації посилення безпеки хостів у локальній мережі. Розглянуто їх переваги та недоліки, а також причину створення власного рішення для автоматизації.

У другому розділі було описано кращі практики провадження автоматизації та віртуальне середовище для тестування проєкту. Також там

детальніше розглянуто розроблений проєкт, додані модулі, створені файли та застосування й налаштовування проєкту і віртуального середовища.

У третьому розділі наведено опис інструментів, завдяки яким було створено цей проєкт та віртуальне середовище.

У четвертому розділі розглянуто ліпші політики безпеки, наведено короткий перелік авторитетних джерел, що створюють ці політики, а також розглянуто застосовані у якості модулів політики безпеки.

У дипломній роботі було виконано наступні завдання:

1)Розглянуто наявні засоби для автоматизації посилення безпеки хостів;

2)Створено віртуальне середовище для розробки та тестування проєкту;

3)Розглянуто та імплементовано у вигляді модулів критичні політики безпеки для ОС CentOS7;

4)Розроблено проєкт для автоматизації посилення безпеки ОС;

5)Протестовано проєкт у віртуальному середовищі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. БлиновА.М. Информационная безопасность / А.М. Блинов. – СПб.: Изд-воСПбГУЭФ, 2010.

2. 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).

3. Вебсайт https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-hardening_your_system_with_tools_and_services

4. Вебсайт https://developer.ibm.com/technologies/linux/articles/l-harden-desktop/

5. Вебсайт https://dev-sec.io/

6. Вебсайт https://documentation.its.umich.edu/node/1119

7. Вебсайт https://galaxy.ansible.com/dev-sec/os-hardening

8. Вебсайт https://github.com/grapheneX/grapheneX

9. Вебсайт https://madaidans-insecurities.github.io/guides/linux-hardening.html

10. Вебсайт https://opensource.com/tags/linux

11. Вебсайт https://security.uconn.edu/server-hardening-standard-windows/#

12. Вебсайт https://securitytrails.com/blog/security-automation

13. Вебсайт https://www.ansible.com/

14. Вебсайт https://www.centos.org/

15. Вебсайт https://www.linux.com/news/9-ways-harden-your-linux-workstation-after-distro-installation/

16. Вебсайт https://www.redhat.com/en/topics/automation/what-is-security-automation

17. Вебсайт https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/

18. Вебсайт https://www.ubuntupit.com/best-linux-hardening-security-tips-a-comprehensive-checklist/

19. Вебсайт https://www.vagrantup.com/

20. Вебсайт https://www.virtualbox.org/

21. 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.

22. 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.

23. 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.

24. ГорбенкоІ.Д. Прикладнакриптологія. Теорія. Практика. Застосування / І.Д. Горбенко, Ю.І. Горбенко. – Х.:Форт, 2012.

25. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі / І. Діордіца // Адміністративне право і процес. – 2017.

26. ДомаревВ.В. Безопасность информационных технологий. Методология создания систем защиты / В.В. Домарев. – К.: ООО "ТИД "ДС", 2002

27. Захист інформаційних ресурсів від атак через Інтернет. Юридична фірма «Partners».− [Електронний ресурс].− Режим доступу: http://partners.kiev.ua/pobudova-sistemi-korporativnoyi-bezpeki/zahist-informatsiynih-resursiv-vid-atak-cherez-internet/.

28. Информационная война и защита информации. Словарь основных терминов и определений. – http://www.csef.ru/files/csef/articles/2176/2176.pdf

29. Піскорська Г. А. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки / Г. А. Піскорська, Н. Л. Яковенко // Міжнародні відносини. Серія «Політичні науки». – 2018. – № 18–19 [Електронний ресурс]. – Режим доступу : http://journals.iir. kiev.ua/index.php/pol_n/article/view/3389.

30. Синадский Н. И. Защита информации в компьютерных сетях: учебное пособие / Н. И. Синадский. – Екатеринбург: УрГУ, 2008.

31. Трофименко О. Г. Законодавча база забезпечення кібербезпеки держави / О. Г. Трофименко // Кібербезпека в Україні: правові та організаційні питання : матер. ІІ Всеукр. наук.-практ. конф. (17 листопада 2017 р.). – Одеса : ОДУВС. – С. 55–56.

32. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005.

33. Шляхи захисту інформаційних ресурсів від несанкціонованого доступу. − [Електронний ресурс].− Режим доступу: http://www.rusnauka.com/13_NMN_2011/Informatica/4_85740.doc.htm

34. Як захистити свій комп’ютер від хакерських атак. Поради Кіберполіції.− [Електронний ресурс].− Режим доступу: http://ranok.ictv.ua/2017/06/28/yak-zahystyty-svij-komp-yuter-vid-hakerskyh-atak/

35. 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).

36. Joseph MacMillan - Infosec Strategies and Best Practices: Gain proficiency in information security using expert-level strategies and best practices - 2021

37. Marvin Waschke - Personal Cybersecurity: How to Avoid and Recover from Cybercrime.

38. Morey J. Haber - Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution.

39. 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. International Conference on Perspective Technologies and Methods in MEMS Designthis, 2019, pp. 32–36, 8817385.

40. 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.

41. 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.

42. Radhi Shatob - Penetration Testing : Step-By-Step Guide

43. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., and Youman, C.E. Role-based access control models. Computer, 29:38-47, Feb. 1996.