камера авто кілька разів побачить одну і ту ж пляму, її реакція буде кожен раз особливою. Зрозуміло, вчені і програмісти з часом вирішать цю проблему, але поки вона залишається.

Підводячи підсумок, можна сказати, що завдяки стрімкому розвитку інформаційних технологій (картографічна сфера, штучний інтелект) безпілотні автомобілі в найближчі 5-15 років стануть невід'ємною частиною нашого життя.

Список літератури

1. Top auptilot electro-car companie». EnergySage: веб-сайт. URL: https://www.energysage.com/electric-vehicles/buyers-guide/top-ev-companies/ (дата звернення 19.04.2020)

2. Omar Hatamle, NASA «We are working on technologies that will compete with people for jobs» NaChasi: веб-сайт. URL: https://nachasi.com/2017/09/08/omar-hatamle/ (дата звернення 16.04.20)

3. Ілон Маск «Tesla отримають повний автопілот до кінця року». Технот: веб-сайт. URL: https://tehnot.com/ua/tesla-poluchat-polnyj-avtopilot-do-kontsa-goda-ilon-mask/ (дата звернення 16.04.2020)

4. Gurney, Jeffrey K. «Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles». Social Science Research Network: веб-сайт. URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2352108 (дата звернення 20.04.2020)

5. Tim Worstall «When Should Your Driverless Car From Google Be Allowed To Kill You?» Forbes: веб-сайт. URL: https://www.forbes.com/sites/timworstall/2014/06/18/when-should-your-driverless-car-from-google-be-allowed-to-kill-you/#11c6dca5fa5b (дата звернення 20.04.2020)

6. Georgia Tech «Hackers Could Use Connected Cars to Gridlock Whole Cities» Horizons: веб-сайт. URL: https://rh.gatech.edu/news/623759/hackers-could-use-connected-cars-gridlock-whole-cities (дата звернення 20.04.2020)

УДК 004.056

Горобець Б. А., студент 4 курсу спеціальності 122 «Комп'ютерні науки та інформаційні технології»
Заплатинська А. О., студентка 4 курсу спеціальності 122 «Комп'ютерні науки та інформаційні технології»
Антонов Ю. С., к.ф.-м.н., доцент, доцент кафедри інформаційних технологій

ПЕРЕВІРКА СИСТЕМИ НА ВРАЗЛИВОСТІ З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ KALI LINUX

Донецький національний університет імені Василя Стуса, м. Вінниця

Тестування на проникнення – це детальний аналіз мережі і систем з точки зору потенційного зловмисника. Суть тесту полягає в санкціонованій спробі обійти існуючий комплекс засобів захисту інформаційної системи. Дані, отримані в результаті успішного тесту на проникнення, часто виявляють

проблеми, які жоден огляд архітектури чи оцінка вразливості не зможуть визначити.[1]

Конфіденційна інформація підприємства (електронні пошти, паролі до облікових записів, реквізити доступу до серверів, хеш-дані облікових записів користувачів та інша інформація, якої немає у відкритому доступі) є метою для багатьох кіберзлочинців. Проблема визначення та аналізу вразливості інформаційної безпеки в корпоративних інформаційних системах є актуальною на сьогоднішній день. Дослідження даного питання дає можливість визначити та класифікувати можливі загрози та модернізувати існуючі або розробити нові ефективні методи та заходи інформаційної безпеки [2].

Згідно останніх досліджень було визначено , що хибне уявлення про безпеку є найбільш вразливою категорією, і зараз вже третій рік поспіль. Проаналізувавши останні дані стало зрозумілим, що 30,1% помилок безпеки були в заголовках безпеки; 28,5% в налаштуваннях додатків; 12,7% в налаштуванні шифрування; 11,5% в конфігурації сервера; 9,6% в налаштуванні мобільного зв'язку; 4,9% в налаштуваннях хмар; і 2,9% через неправильне контролю безпеки [3].

Метою даної роботи є дослідження інструментів Kali Linux з метою виявлення вразливостей для покращення рівня безпеки системи.

Оцінка вразливості є одним з найбільш важливих етапів тестування на проникнення. Аналіз вразливостей досить схожий на збір інформації, але на цей раз у нас є дуже конкретна мета - знайти слабкі місця, які можуть бути успішно використані зловмисником. Цей етап відіграє вирішальну роль в тестуванні проникнення, тому що в більшості випадків вразливість робить вашу систему або продукт схильним до кібератак.

Під час тестування на проникнення особливу увагу слід приділяти різним проблемам і можливим векторах атаки:

- Збір інформації
- Аналіз вразливих місць
- Sniffing і Spoofing
- Стрес-тестування

На початку тестування продукту на проникнення, перше, що вам потрібно зробити, це зібрати якомога більше інформації про систему. Цей етап дозволяє вам побачити, чи може тестована система бути досліджена зовні і чи можуть потенційні зловмисники витягти будь-які критичні дані. Наприклад, інформація про технології, порти, протоколи, версії програмного забезпечення, точки входу та архітектуру продукту може значно збільшити шанси успіху чи атаки. Ваша мета - захистити цю інформацію, або, хоча б, вкрай ускладнити для потенційного зловмисника витяг такої інформації з вашого продукту.

Після оцінки вразливості, ми можемо перейти до такої ж цікавої і важливою стадії: відстеження трафіку і спуфінг трафіку. Одним з основних застосувань є виявлення мережевих вразливостей і слабких місць, які можуть бути мішенню для атакуючих. Ви можете перевірити шляхи, по яких пакети

передаються у вашій мережі, і подивитися, куди і кому передаються пакети, яку інформацію вони містять, чи зашифровані вони.

Kali Linux є потужним і надзвичайно корисним інструментом. Хоча він пропонує вражаюче багатий набір інструментів для кожного етапу процесу тестування проникнення, остаточний вибір інструментів завжди буде залежати від завдань і цілей вашого поточного проекту. При різних обставинах одні і ті ж інструменти можуть демонструвати абсолютно різні рівні точності і ефективності.

Тестування проникнення є практикою тестування комп'ютерної системи, мережі або веб-додатків для пошуку вразливостей безпеки, які атакуючий може використовувати. Тестування на проникнення здійснюється з використанням методів і засобів, що використовуються кіберзлочинцями, для того щоб виявити ці вразливі місця, але вони уповноважені робити це. Це означає, що на відміну від кіберзлочинця тестер проникнення має дозвіл організації, яка проходить тестування.

Проблеми, спричинені неохайною системою адміністрування та поспішаючими реалізаціями, часто становлять серйозну загрозу для організації, тоді як рішення відпадають під десяток елементів у списку справ адміністратора. Тестування на проникнення підкреслює ці неправильно визначені пріоритети та визначає, що потрібно зробити організації, щоб захиститися від реального вторгнення.

На даний час Kali Linux пропонує найкращі в світі комплекти для зломів і тестування проникнення. У цій статті ми говорили про те, як можна використовувати Kali Linux для тестування проникнення.

Список літератури

1. David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni,Metasploit: The Penetration Tester's Guide, 2011. с 13-14

2. Дмитро Мехед, Юлія Ткач, Володимир Базилевич, Володимир Гур'єв, Ярослав Усов, Аналіз вразливостей корпоративних інформаційних систем,Том 20, 2018

3. Caroline Wong and Joe Sechman. The State of Pentesting 2019, 2019, URL: http://resource.cobalt.io/the-state-of-pentesting-2019.

УДК 004.732:338.48

Дем'янюк Л. С., студентка 4 курсу спеціальності 122 «Комп'ютерні науки та інформаційні технології»
Нескородєва Т. В., к.т.н., доцент, доцент кафедри інформаційних технологій

РОЗРОБКА АВТОМАТИЗОВАНОЇ ПІДСИСТЕМИ ОБЛІКУ ТА АНАЛІЗУ ТУРІВ І ПУТІВОК ТУРИСТИЧНОЇ ФІРМИ

Донецький національний університет імені Василя Стуса, м. Вінниця