DOI:10.18372/2310-5461.46.14807

УДК 681.3.06

Л. П. Галата
Національний авіаційний університет
orcid.org/0000-0002-7978-3954
e-mail: galataliliya@gmail.com;

Б. Я. Корнієнко, д-р. техн. наук, доц.
Національний технічний університет України
«Київський політехнічний інститут імені І.Сікорського»
orcid.org/0000-0002-2521-0878
e-mail: bogdanko@gmx.net

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ GNS3

Вступ

Корпоративні мережі на сьогодні займають значну частину інфраструктури компаній як IT-напрямку так і компаній інших виробничих чи сервісних галузей. Не можливо уявити компанію без найменшої, хоча б локальної, мережі. Сполучення робочих станцій та серверів у мережу обміну інформацією дозволяє синхронізувати працю декількох людей, офісів, компаній та навіть країн. Переоцінити вплив корпоративних мереж дуже важко.

Але під час передачі, зберігання, обчислення тощо, інформації виробничі компанії стикаються з проблемою, яка присутня завжди, якщо в локальній чи глобальній мережі присутній обмін інформацією між станціями, мережевими сегментами або власне мережами. Проблема захисту інформації в корпоративних мережах стоїть дуже гостро, тому що в сучасному світі порушення безпеки інформації може призвести до серйозних наслідків та мільйонних збитків для корпорацій. Так пошкодження інформації при передачі між мережами чи її сегментами може призвести до фатальних наслідків, якщо це виміри від яких залежить точність подальших обчислень. Затримка передачі інформації чи її доступність також відіграють важливу роль, коли система повинна реагувати на зовнішній чи внутрішній збудник і формувати пакет даних для миттєвого відгуку. Особливо небезпечними для комп'ютерних мереж є зловмисники, спеціалісти, професіонали в сфері обчислювальної техніки, які досконало володіють знаннями всіх переваг та слабких сторін обчислювальних мереж та систем і мають найсучасніші інструментальні та технологічні ресурси для аналізу та злому механізмів захисту корпоративних мереж. Дотримання правил захисту інформації не завжди допомагає в захищенні мережі. Корпоративні мережі висувають потребу в дослідженні нових методів захисту. Реалізації методів, алгоритмів, систем, які захищають важливі дані від стороннього несанкціонованого втручання легко знайдуть свого споживача [1–4].

Постановка проблеми

Проблема захисту інформації виникла через створення спільного інформаційного простору і застосування комп'ютерів і комп'ютерних мереж у всіх сферах життя і життєдіяльності. Захист інформації в комп'ютерних системах повинен бути зрозумілим для регулярного використання інструментами і методами захисту, вжиття заходів із забезпечення системи достовірності інформації, що зберігається і оброблюється в комп'ютерних системах [5–6]. Під об'єктом захисту виступає інформація чи її носій або інформаційний процес, щодо якого ви хочете встановити бажаний, виходячи з розв'язуваної проблеми, рівень безпеки. Електронний захист інформації запобігає наступним видам інформаційних загроз: відстеження інформації, несанкціонований доступ неавторизованих користувачів, неправильне використання, пошкодження, руйнування, спотворення, копіювання, блокування. З метою забезпечення захисту від вищевказаних загроз, комп'ютерна система повинна здійснювати захист для: носіїв інформації, технічних засобів обробки, засобів передачі, методів обробки, баз даних. Інформаційна безпека це захист інформації від незаконного ознайомлення, трансформації та знищення, а також захист ресурсів від впливу,

спрямованого на порушення їх уміння працювати. Інформаційна безпека досягається за рахунок забезпечення конфіденційності, цілісності і надійності оброблюваних даних, а також доступності і цілісності компонентів і ресурсів комп'ютерної системи [7–9]. Серед найбільш поширених і найбільш частих веб-атак є XSS (міжсайтовий скриптинг) і SQL-ін'єкція. При розробці системи захисту інформації в корпоративній мережі головним завданням було розробити систему захисту, яка була б стійкою до зазначених веб-атак.

Аналіз останніх досліджень і публікацій

Перед початком планування та розробки власної реалізації, розглянемо декілька варіантів існуючих рішень у галузі захисту інформації корпоративних мереж [10–15].

Веб-сервіс Webroot Secure Anywhere Endpoint Protection.

Webroot Secure Anywhere Endpoint Protection забезпечує багатовекторний захист від вірусів і шкідливих програм, що надають повний захист від усіх сучасних шкідливих загроз, включаючи трояни, клавіатурні шпигуни, фішинг, шпигунські програми, зворотні двері, руткіти, нульові та постійні загрози. Вбудований ідентифікаційний і конфіденційний щит припиняє крадіжку або захоплення даних при використанні Інтернету, а вихідний брандмауер також зупиняє злодійські дані. Немає необхідності турбуватися або запускати оновлення — засоби безпеки, керовані хмарою, кінцеві точки завжди актуальні. Можна зробити висновки, що даний додаток не має універсальності і великої швидкості вбудовування в систему.

Manage Engine Firewall Analyzer. Firewall Analyzer є агентом лог-аналітики і управління конфігурацією програмного забезпечення, яке аналізує логи з брандмауерів і генерує сповіщення в режимі реального часу, оповіщення безпеки і пропускної здатності звітів. Він також надає можливість адміністраторам надавати вичерпні звіти про події безпеки і, в свою чергу, вони можуть вживати заходів для пом'якшення безпеки.

Можливості мережної безпеки:

— перегляд повного списку програмного забезпечення мережної безпеки;

— антиспам;

— антивірус;

— захист електронної пошти;

— відстеження подій;

— система виявлення вторгнень;

— IP захист;

— відповідь на загрозу;

— сканування вразливості;

— управління веб-загрозами;

— звітність про веб-трафік.

Окрім завантаження, встановлення та вибору бажаної підтримуваної бази даних, даний додаток не потребує додаткових конфігурацій, що є надзвичайним плюсом.

Отже підводячи підсумки, Mange Engine дуже гнучкий додаток, з різноманітними можливостями налаштування основною задачею якого є вбудування Firewall-ів в існуючі системи і аналіз трафіку.

Мета статті — представлення власної реалізації рішення в галузі захисту інформації корпоративних мереж, мета якої забезпечити захист від одних з найбільш поширених веб-загроз, а саме SQL Injection та Cross-site scripting.

Виклад основного матеріалу дослідження

Для даної системи вирішено розробити програмний пакет за допомогою технології ASP.NET Core.

Програмний пакет складатиметься з чотирьох взаємодіючих між собою компонентів. Для цього архітектура додатку реалізовуватиметься за допомогою патерну «мікросервісної архітектури».

Як вже було визначено система захисту буде складатися з чотирьох компонентів захисту:

1) Gateway на основі реверсивного проксі-сервера.
2) Firewall.
3) Logger.
4) Digital Signature Verifier.

Елементи, які дозволять протестувати систему захисту як цілісну імітаційну модель:

1) Internet.
2) Kali Linux.
3) Corporate Network.

Загальний вигляду робочої системи наведено на рис. 1.

Розглянемо кожен елемент системи захисту, його роль, функції та реалізацію.

Елемент системи Internet.

Компонент системи Internet — саме з цього елементу під час симуляції імітаційної моделі в GNS3 будуть намагатися пройти, згенеровані за допомогою програмного пакету Kali Linux, загрози в нашу корпоративну мережу. Компонент Internet відіграє роль зловмисника, атакуючого корпоративну мережу (рис. 1).

Функції даного елементу системи захисту зрозумілі, генерація загроз та спроби надсилання загроз на *endpoint* корпоративної мережі [16–18].

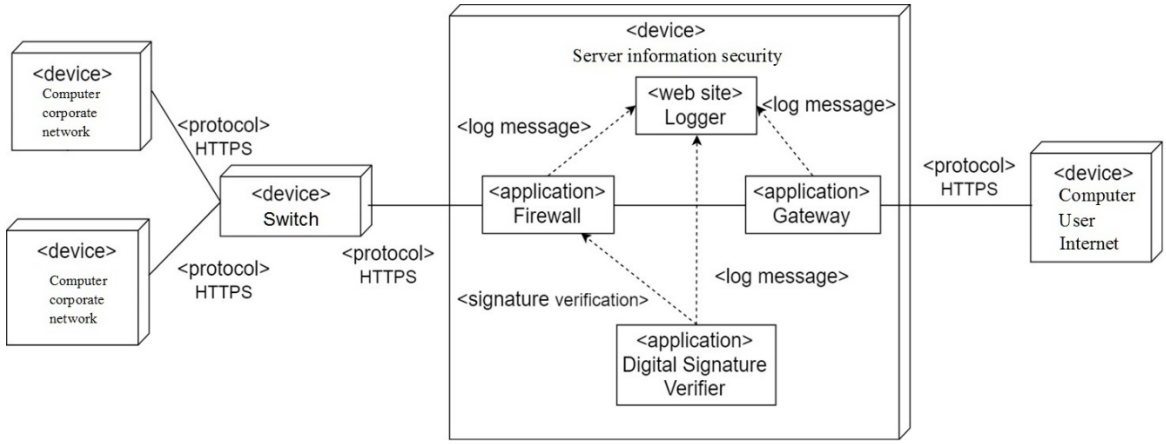

Рис. 1. Система захисту інформації корпоративної мережі

Реалізація даного компоненту взята з готового програмного пакету в Kali Linux. Для імітації атакуючої сторони було обрано програму Vega Usage. Дана програма імітує загрози наступних типів:

1) XSS (Cross Site Scripting);
2) SQL Injection.

Елемент системи Kali Linux.

Даний елемент виконує роль генератора загроз обраних типів. Проведено стрес-тестування розробленої системи захисту за допомогою програми Vega Usage, яка генерує загрози (XSS, SQL Injection).

Елемент системи захисту Gateway.

Даний елемент, розроблений з використанням reverse-proxy програмного дизайну, виконує роль реверсивного проксі-серверу, який буде перенаправляти запити на *endpoint* корпоративної мережі.

Реверсивний проксі-сервер — це сервер, який розташований перед веб-серверами і пересилає клієнтські (наприклад, веб-браузер) запити до цих веб-серверів.

Зворотні проксі, як правило, реалізуються для підвищення безпеки, продуктивності та надійності.

Функціями Gateway є розпізнавання та трактування web-запиту до одного з endpoint, фільтрація нерозпізнаних, некоректних чи з загрозливим вмістом запитів на endpoint корпоративної мережі.

Алгоритм формування електронно-цифрового підпису.

В проекті використовується цифровий підпис для підсилення системи захисту корпоративної мережі від проникнення зловмисних web-запитів.

Реалізовано алгоритм формування цифрового підпису та його перевірку при надходженні запиту на мікросервіс Digital Signature Verifier.

Елемент системи захисту Logger.

Останнім компонентом системи захисту є мікросервіс логування. Основна роль даного елементу є запис усіх дій що відбуваються під час надходження та проходження веб-запиту крізь систему захисту. Цей мікросервіс надає можливість переглядати інформацію стосовно прийнятого запиту та усіх дій або заходів, якщо це виявився загрозливий запит, які були застосовані для його подальшого проходження до корпоративної мережі. Основними функціями даного компоненту є запис (логування) усіх дій над запитом, конвертаціями, читанням та фільтрацією запитів, які надходять з мережі Інтернет в систему захисту. Логер дозволить зібрати статистику та проаналізувати продуктивність розробленої системи захисту. Аналіз потужності захисту дозволить в подальшому виділити слабкі місця захисту та розробити покращення. Даний мікросервіс є додатком типу Web API і приймає запити на логування від інших мікросервісів системи захисту. Також даний мікросервіс є універсальним до прийому логуючих повідомлень. Так у разі розширення кількості мікросервісних компонентів, вони також з легкістю будуть під'єднані до системи захисту.

Конфігурація Kali Linux та реалізація проекту.

Для виконання цілей атакуючої сторони, було обрано програмну операційну систему Kali Linux, вона містить широкий спектр програм та віджетів для зловмисних атак. Після встановлення Virtual Box, встановлено Kali Linux на віртуальну машину.

Створено три хости в Virtual Box:

1) Хост Kali Linux.
2) Хост ПК на якому буде запущена система захисту.
3) Хост Ubuntu зі встановленим GNS3.

Хост Kali Linux потрібен для того, щоб під'єднати його за допомогою інструментів віртуальної машини в середину топології, яка побудована в GNS3. На даному хості встановлена Kali Linux операційна система, на ній запущено програмний пакет Vega Usage.

Vega Usage є сканером і тестовою платформою з відкритим кодом для перевірки безпеки веб-додатків. Vega допомагає знайти та перевірити SQL Injection, Cross-Site Scripting (XSS), розкривши конфіденційну інформацію та інші уразливості. Він працює на Linux і Windows.

Vega включає в себе автоматизований сканер для швидких тестів і перехоплюючий проксі для тактичної перевірки. Vega може бути розширена за допомогою потужного API на JavaScript.

Для реалізації проекту обрано пакет GNS3. GNS3 – це графічний емулятор мережі, який дозволяє моделювати віртуальну мережу з мережевого обладнання більше ніж 20 різних виробників на локальному комп'ютері, приєднувати віртуальну мережу до реальної, додавати в мережу повноцінний комп'ютер, підтримується сторонні програми для аналізу мережевих пакетів, зокрема Wireshark [19–20]. Також наявна підтримка утиліти SolarWinds Response Time Viewer, яка приймає на вхід збережені дампи трафіка і аналізує час відклику мережі і об'єми переданих даних, а також представляє які додатки і ресурси були виявлені в дампі, що піддавався аналізу. Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережних операційних систем. Для зручності тестування відразу після встановлення реалізована підтримка програм для віртуалізації, що дозволяє додати в мережу віртуальну машину і проводити відповідні тести мережі, зокрема VMware та VirtualBox. GNS3 є фактично графічною оболонкою для Dynamips, також є повноцінна підтримка QEMU і Cisco IOU, тому успадковує всі переваги і недоліки кожної із технологій [21–23]. Після конфігурації та налаштування компонентів мережі в GNS3 одержимо результат (рис. 2).

Під час запуску проекту реалізовано Kali Linux та програму Vega.

Серед загроз обрано дві — Cross-Site Scripting та SQL Injection (рис. 3). Вибравши один з надісланих загрозливих запитів, можна розглянути детальну інформацію про згенерований запит та яку конкретно загрозу він містив у собі (рис. 4). Реакція системи захисту інформації корпоративної мережі наведена на рис. 5, 6. Ведення логів здійснено за допомогою Logger мікросервісу.

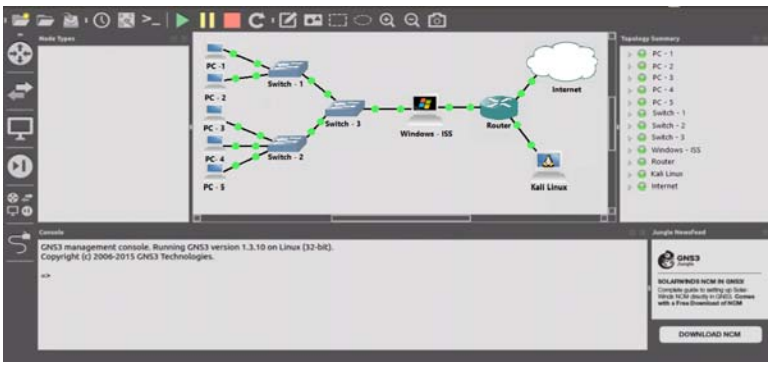

Рис. 2. Робоча поверхня GNS3 з налаштованою імітаційною мережею

Рис. 3. Вибір загроз у програмі Vega

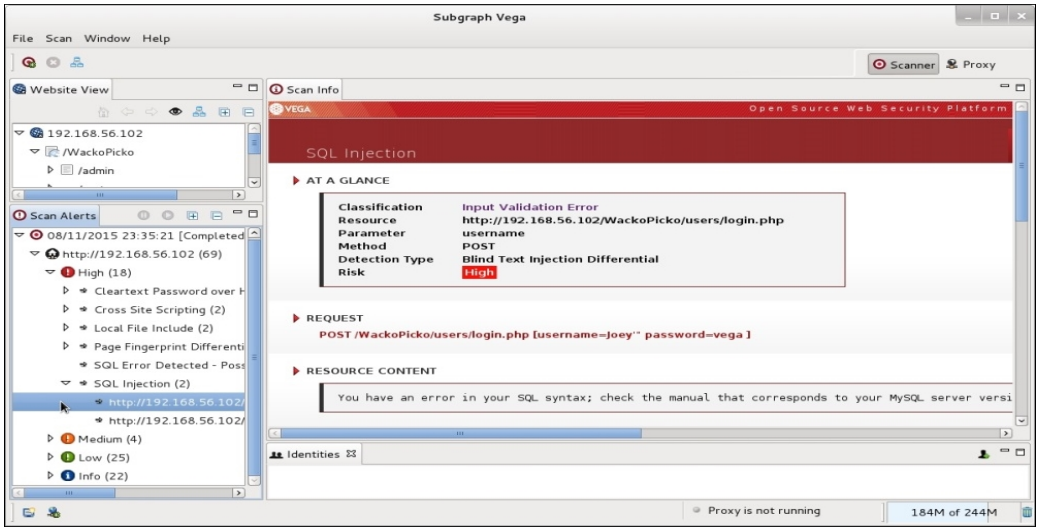

Рис. 4. Основна інформація про надісланий загрозливий запит

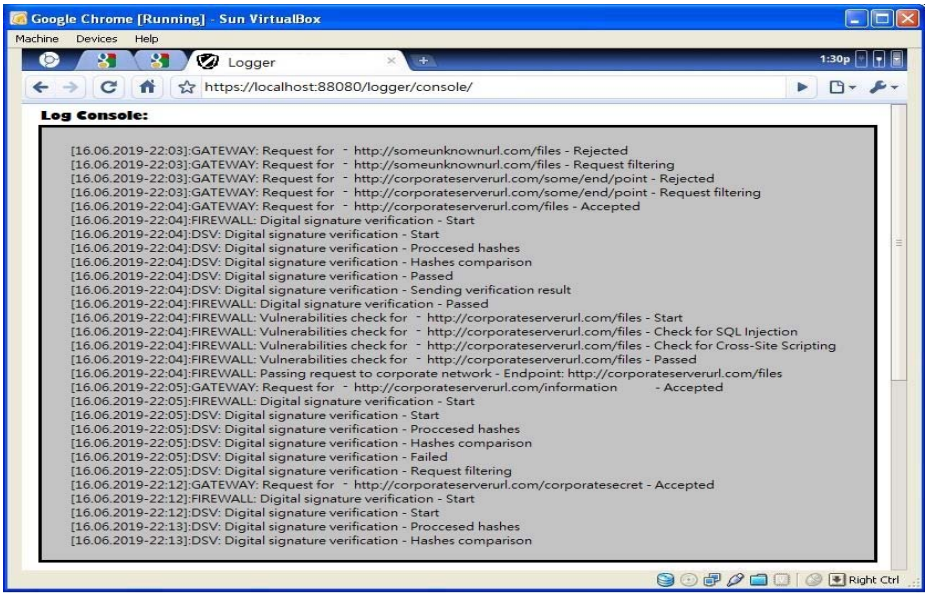

Рис. 5. Реакція системи захисту інформації у вікні мікросервіса Logger

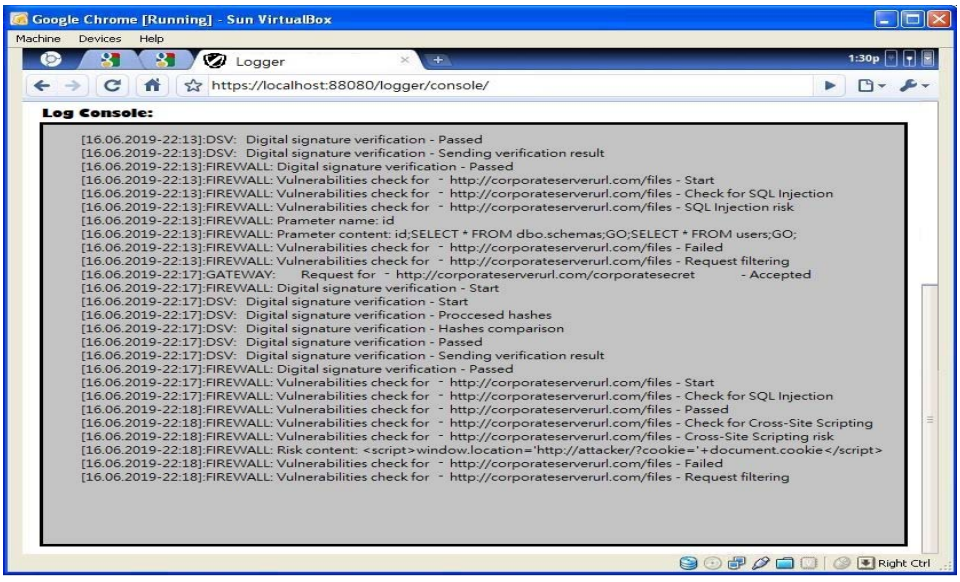

Рис. 6. Виявлення атак системою захисту інформації

На цьому симуляцію атак завершено. Обидві атаки виявлено та нейтралізовано. Проаналізувавши статистичні дані можна зробити висновки щодо ефективності розробленої системи захисту інформації в корпоративній мережі.

Висновки

У результаті виконання дослідження розроблено систему, яка складається зі спільно взаємодіючих між собою мікросервісів (Gateway, Firewall, Digital Signature Verifier та Logger), ціль якої забезпечити захист від одних з найбільш поширених веб-загроз, а саме SQL Injection та Cross-site scripting.

Оскільки основною технологією розробки є ASP.NET Core фреймворк, система може бути розгорнута на усіх операційних системах, які на даний момент підтримують ASP.NET Core (Windows, Linux, macOS). Система є повністю автономною. Після встановлення необхідних інструментальних додатків на комп'ютер або сервер система відкриває доступ тільки до Logger API. Дане API забезпечує доступ на сторінку ведення логів, на цій сторінці присутня повна звітність від моменту, коли веб-запит надійшов до Gateway, до моменту відправлення запиту до корпоративної мережі. Перевірка цифрового підпису забезпечує додатковий шар захисту і запобігає атакам, які відтворені в наслідок витоку інформації або витоку інформації за допомогою інсайдерів endpoint корпоративної мережі. Запити, які влучили в один з зареєстрованих endpoint-ів і пройшли далі до Firewall-у будуть відсіяні на етапі перевірки цифрового підпису.

Проведені стрес тестування за допомогою програми Vega (Kali Linux) показують, що система надзвичайно стійка до атак типу XSS та SQL Injection. Розроблена система захисту має перспективи для подальшого ускладнення захисних механізмів або побудови додаткових шарів захисту наприклад, декілька ЕЦП, окремий мікросервіс для усунення та фільтрації загрозливих запитів будь-якого типу.

ЛІТЕРАТУРА

1. Курилов Ф. М. Моделирование систем защиты информации. Приложение теории графов. Технические науки: теория и практика: материалы III Междунар. науч. конф. Чита: Издательство Молодой ученый. 2016. С. 6–9.

2. Росенко А. П. Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации: монографія. М.: Гелиос АРВ, 2008. 154 с.

3. Корнієнко Б. Я. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. *Моделювання та інформаційні технології*. 2018. Вип. 83. С. 34–41.

4. Корнієнко Б. Я. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. *Наукоємні технології*. 2017. № 4 (36). С. 316–322.
DOI: 10.18372/2310-5461.36.12229

5. Korniyenko B., Yudin A., Galata L. Risk estimation of information system. Wschodnioeuropejskie *Czasopismo Naukowe*. 2016. № 5. P. 35–40.

6. Корнієнко Б. Я., Юдін О. К., Снігур О. С. Безпека аутентифікації у web-ресурсах. *Захист інформації*. 2012. № 1 (54). С. 20–25.
DOI: 10.18372/2410-7840.14.2056 (ukr).

7. Корнієнко Б. Я., Максімов Ю. О., Марутовська Н. М. Прикладні програми управління інформаційними ризиками. *Захист інформації*. 2012. № 4 (57). С. 60–64.
DOI: 10.18372/2410-7840.14.3493 (ukr).

8. Galata, L., Korniyenko, B., Yudin, A.: Research of the simulation polygon for the protection of critical information resources. In: CEUR Workshop Proceedings, Information Technologies and Security, Selected Papers of the XVII International Scientific and Practical Conference on *Information Technologies and Security* (ITS 2017), 30 Nov 2017, Kyiv, Ukraine. Vol. 2067. Pp. 23–31, urn:nbn:de:0074-2067-8.

9. Raphael Hertzog, Jim O'Gorman, and Mati Aharoni. Kali Linux Revealed. Offsec Press, 2017. 347 p.

10. Lei Chen, Hassan Takabi, Nhien-An Le-KhacJohn Wiley & Sons. Security, Privacy, and Digital Forensics in the Cloud, 2019. 360 p.

11. Glen D. Singh, Rishi Latchmepersad. CompTIA Network+ Certification Guide, 2018. 422 p.

12. Dijiang Huang, Ankur Chowdhary, Sandeep Pisharody. Software-Defined Networking and Security: From Theory to Practice, 2018. 328 p.

13. Robert M. Lee. Active Cyber Defense Cycle, 2016. 651 p.

14. Jason C. Neumann, The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More 1st Edition, 2015. 274 p.

15. Kwangjo Kim, Muhamad Erza Aminanto, Harry Chandra Tanuwidjaja. Network Intrusion Detection Using Deep Learning: A Feature Learning Approach, 2018. 79 p.

16. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources. CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "*Information Technologies and Security*" (ITS 2018) Kyiv, Ukraine, November 27, 2018. Vol. 2318. Pp. 176–187. urn:nbn:de:0074-2318-4.

17. Kravets, P., Shymkovych, V.; Hardware Implementation Neural Network Controller on FPGA for Stability Ball on the Platform 2nd International

Conference on Computer Science, *Engineering and Education Applications*, ICCSEEA 2019; Kiev; Ukraine; 26 January 2019 – 27 January 2019 (Conference Paper). Volume 938. Pp. 247–256.

18. Kravets P. I., Shymkovych V. M. and Samo tyy V. Method and technology of synthesis of neural network models of object control with their hardware implementation on FPGA. Proceedings of the 2017 IEEE 9th International Conference on *Intelligent Data Acquisition and Advanced Computing Systems*: Technology and Applications (IDAACS). 2017. Vol. 2. Pp. 947–951.

19.Samotyy V., Telenyk S., Kravets P., Shymkovych V. and Posvistak T. "A real time control system for balancing a ball on a platform with FPGA parallel implementation", *Technical Transactions*. 2018. vol. 5. Pp. 109–118.

20. Arber B. and Davey, J. The use of the CCTA risk analysis and management methodology CRAMM. Proc. MEDINFO92. North Holland. 1992. Pp. 1589–1593.

21. Ryabko B. Y., Monarev V. A. Using information theory approach to randomness testing. Journal of *Statistical Planning and Inference*. 2005. Vol. 133. № 1. Pp. 95–110.

22. Chris Clymer, Ken Stasiak, Matt Neely, Stephen Marchewitz. IRisk Equatuion Available via https://securestate.en/iRisk-Equation-Whitepaper.pdf

23. Common Vulnerability Scoring System v 3.0: User Guide. Available via https://www.first.org/cvss/user-guide

Галата Л. П., Корнієнко Б. Я.

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ GNS3

Проведено дослідження системи захисту інформації корпоративної мережі на основі GNS3. Побудована імітаційна модель системи захисту корпоративної мережі на базі GNS3. Програма GNS3 – графічний емулятор мережі, який дозволяє моделювати віртуальну мережу з мережного обладнання більше ніж двадцяти різних виробників на локальному комп'ютері, приєднувати віртуальну мережу до реальної мережі. Система захисту інформації корпоративної мережі складається з мікросервісів Gateway, Firewall, Digital Signature Verifier та Logger. Використано елементи, які дозволять протестувати систему захисту як цілісну імітаційну модель. Розроблено програмний пакет за допомогою технології ASP.NET Core. Архітектура додатку реалізована за допомогою патерну проектування «мікросервісної архітектури». Розглянуто кожен елемент системи захисту, його роль, функції та реалізацію. Реалізовано захист від загроз SQL Injection та Cross-site scripting. Перевірка цифрового підпису забезпечує додатковий шар захисту інформації. Представлена реакція системи захисту інформації корпоративної мережі на надісланий загрозливий запит. Проаналізовано ведення логів за допомогою Logger мікросервісу, аналіз потужності захисту дозволить в подальшому виділити слабкі місця захисту та розробити покращення. Проведені стрес тестування за допомогою програми Vega (для виконання цілей атакуючої сторони, було обрано програмну операційну систему Kali Linux) показали, що система надзвичайно стійка до атак типу SQL Injection та Cross-site scripting. Розроблена імітаційна модель системи захисту корпоративної мережі на базі GNS3 із використанням цифрового підпису мінімального розміру із забезпеченням заданого рівня стійкості. Проаналізовано статистичні дані щодо реакції системи захисту інформації. Зроблено висновки щодо ефективності розробленої системи захисту інформації в корпоративній мережі.

Ключові слова: математична модель; загроза; система захисту; критичні інформаційні ресурси.

Galata L., Korniyenko B.

RESEARCH OF THE CORPORATE NETWORK INFORMATION PROTECTION SYSTEM BASED ON GNS3

A study of the information protection system of a corporate network based on GNS3 was performed. A simulation model of the corporate network protection system based on GNS3 has been built. The GNS3 program is a graphical network emulator that allows you to simulate a virtual network that consists of network equipment of more than twenty different manufacturers on a local computer, and connect a virtual network to a real network. The corporate network information protection system consists of Gateway, Firewall, Digital Signature Verifier and Logger microservices. We used elements that will allow us to test the protection system as a complete simulation model. A software package was developed using ASP.NET Core technology. The application architecture is implemented using the design pattern of "microservice architecture". Each element of the protection system, its role, functions and implementation are considered. SQL Injection and Cross-site scripting threat protection was implemented. Digital signature verification provides an additional layer of information security. The response of the corporate network information protection system to a threatened request is presented. Logging was analyzed using the Logger microservice, protection analysis will further identify weak points of protection and develop improvements.

Conducted stress tests using the Vega program (to fulfill the goals of the attacker, the Kali Linux software operating system was chosen) showed that the system is very resistant to attacks such as SQL Injection and Cross-site scripting. A simulation model of the corporate network protection system based on GNS3 using a digital signature of a minimum size with a specified level of stability has been developed. Statistical data on the reaction of the information protection system are analyzed. Conclusions are drawn about the effectiveness of the developed information protection system in the corporate network.

Keywords: mathematical model; threat; system of protection; critical information resources.

Галата Л. П., Корниенко Б. Я.

ИССЛЕДОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНОЙ СЕТИ НА ОСНОВЕ GNS3

Проведено исследование системы защиты информации корпоративной сети на основе GNS3. Построена имитационная модель системы защиты корпоративной сети на базе GNS3. Программа GNS3 - графический эмулятор сети, который позволяет моделировать виртуальную сеть с сетевого оборудования более чем двадцати различных производителей на локальном компьютере, присоединять виртуальную сеть к реальной сети. Система защиты информации корпоративной сети состоит из микросервисов Gateway, Firewall, Digital Signature Verifier и Logger. Использованы элементы, которые позволят протестировать систему защиты как целостную имитационную модель. Разработан программный пакет с помощью технологии ASP.NET Core. Архитектура приложения реализована с помощью паттерна проектирования «микросервисной архитектуры». Рассмотрен каждый элемент системы защиты, его роль, функции и реализация. Реализовано защиту от угроз SQL Injection и Cross-site scripting. Проверка цифровой подписи обеспечивает дополнительный слой защиты информации. Представлена реакция системы защиты информации корпоративной сети на отправленный угрожающий запрос. Проанализировано ведение логов с помощью Logger микросервиса, анализ защиты позволит в дальнейшем выделить слабые места защиты и разработать улучшения. Проведенные стресс тесты с помощью программы Vega (для выполнения целей атакующей стороны, была выбрана программная операционная система Kali Linux) показали, что система очень устойчива к атакам типа SQL Injection и Cross-site scripting. Разработана имитационная модель системы защиты корпоративной сети на базе GNS3 с использованием цифровой подписи минимального размера с обеспечением заданного уровня устойчивости. Проанализированы статистические данные по реакции системы защиты информации. Сделаны выводы об эффективности разработанной системы защиты информации в корпоративной сети.

Ключевые слова: математическая модель; угроза; система защиты; критические информационные ресурсы.

Стаття надійшла до редакції 24.04.2020 р.
Прийнято до друку 08.06.2020 р.