УДК 004.77

БЕЗПЕКА СЕРВЕРНИХ СИСТЕМ. МОДЕЛЮВАННЯ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА

Алексієв В.О.

Харківський національний економічний університет імені Семена Кузнеця,
Харків, просп. Науки, 9-А, 61166 Україна.
E-mail: vlax@hneu.edu.ua

Вступ. Забезпечення безпеки серверних систем слід планувати ще на етапі розгортання окремого серверу [1] чи на стадії формування логічної топології локальної мережі підприємства [2]. На цьому етапі важливо виконати перевірку доцільності та тестування розгортання тієї чи іншої операційної системи і відповідного програмного забезпечення серверних сервісів. Зазвичай, такі дії виконуються у середовищі віртуалізації на комп'ютері системного адміністратора чи DevOps інженера. У цьому випадку, частіше обирають систему VirtualBox (https://www.virtualbox.org/) у якості середовища віртуалізації або ін.

Для побудови моделі серверної інфраструктури на базі системи віртуалізації в обмеженні середовища операційної системи продуктивного комп'ютера, слід звернути увагу на конфігурацію мережевих інтерфейсів віртуальних машин. У разі успішного планування розгортання систем та сервісів це обумовить можливості швидкого розгортання рішення у реальних умовах застосування.

Іншим варіантом створення моделі для тестування і налагодження засобів забезпечення безпеки серверних систем є безпосереднє моделювання у середовищі Cloud Computing, особливо, у разі коли сама серверна інфраструктура підприємства розгорнута у відповідному середовищі. Перевагою такого підходу є те, що розгорнута та протестована віртуальна машина може бути зразу задіяна як одиниця наявної серверної архітектури. Наприклад, для невеликого кластеру віртуалізації у середовищі приватної хмари – це можна реалізувати на базі системи Proxmox VE (https://pve.proxmox.com/) або ін. Однак, такий підхід повинен враховувати, що виконання експерименту пов'язано із необхідністю ізоляції тестового середовища від діючого простору ІТ-середовища підприємства.

Розглянемо особливості організації тестового полігону (кіберполігону) для виконання моделювання серверної інфраструктури підприємства.

Матеріал і результати дослідження. Для віртуальних машин, що будуть виконувати завдання у моделі серверних систем підприємства, необхідним є забезпечення можливості їх мережевої взаємодії один з одним, наприклад, можна застосувати мережу 192.168.1.0/24. Поруч з цим, кожен вузол повинен мати Інтернет-з'єднання для можливості оновлення систем та завантаження необхідних програмних компонентів.

Майже оптимальним для рішення визначеного завдання, у разі застосування системи віртуалізації VirtualBox, є вибір для кожної віртуальної машини типу мережевого адаптеру – «Bridget Adapter» (міст). Це зможе поєднати віртуальну машину та мережевий адаптер комп'ютеру, на котрому працює система віртуалізації (хост-система), своєрідним комутатором (Switch). Тому, гостьова система, на рівні з мережею хост-системи зможе отримати повнофункціональне обслуговування маршрутизатором, який має набір сервісів та зв'язок з мережею Інтернет-провайдеру. Безпеку такого з'єднання віртуальних машин забезпечує налаштування маршрутизатору, при цьому, з основної операційної системи, у середовищі якої працює система віртуалізації, будуть доступні всі гостьові системи.

Однак, не завжди можна застосувати апаратний маршрутизатор у завданнях моделювання мережевої інфраструктури. Наприклад, у разі використання мобільної точки доступу, або можливості отримання з'єднання тільки за однією IP-адресою основної хост-системи тощо. У такому випадку, доцільно для віртуальної машини у середовищі VirtualBox

застосувати адаптер типу «NAT Network». Попередньо у налаштуваннях системи віртуалізації слід додати: «Tools»-«Preferences»-«Network»-«Add new NAT Network» та задати відповідне ім'я мережі, її адресний простір, наприклад, 10.0.2.0/24.

Звичайно, це надає можливості для комунікації всередині мережі всім віртуальним машинам, а за технологією NAT вони отримають доступ до мережі Інтернет. Слід зазначити, що за наявності сервісу NAT буде неможливим отримати доступ із головної операційної системи комп'ютеру (за замовчуванням із віртуальною мережевою картою: 192.168.56.1), на якому працює VirtualBox, до гостьових віртуальних машин. Це може значно ускладнити роботу з моделлю мережі за потреби взаємодії з гостьовою системою за протоколом ssh або, якщо намагатись звернутися до її веб-серверу тощо.

На практиці налагодити мережеву взаємодію між гостьовими операційними системами та основною хост-системою, у якій запущено VirtualBox, можна за допомогою технології перенаправлення портів (Port Forwarding). Перенаправлення портів слід задати у конфігурації «Tools»-«Preferences-Network» для визначеної мережі. Наприклад, для ssh-з'єднання з віртуальною машиною, яка має IP-адресу 10.0.2.100 (Guest IP) та відкритий стандартний порт 22, слід вказати правило перенаправлення на вільний порт хост-системи, наприклад, порт 2222 з IP-адресою 192.168.56.1 (Host IP) за протоколом TCP. Таких правил можна надати будь-скільки за потреби налагодження прозорої комунікації з гостьовими віртуальними машинами. Обмеженням буде тільки пул значень наявних вільних мережевих портів.

Порівняно схожим до моделі на локальному комп'ютері є застосування системи Proxmox VE, яка вже має масштаб рівня центру обробки даних (ЦОД). На її базі можна побудувати кіберполігон для виконання завдань тестування рівня безпеки серверних систем на моделі IT-інфраструктури підприємства. У цьому разі зникають обмеження на роботу з мережевими інтерфейсами відповідно до їх наявності у ЦОД. Однак, у разі побудови зачиненої приватної мережі може виникнути необхідність застосування технології перенаправлення портів, або залучення додаткової віртуальної машини, що має доступ, наприклад до графічного вікна за технологією RDP тощо. Застосування окремої віртуальної машини для доступу у захищену мережу обумовлено характером системи віртуалізації Proxmox VE.

Слід враховувати, що VirtualBox – це, так звана, Desktop-віртуалізація, у якій користувач отримує доступ до графічного вікна гостьової операційної системи. У протилежність до цього, у Server-based віртуалізації (Proxmox VE) забезпечується рішення завдань підтримки швидкодії віртуальних машин та гнучкість налаштування мережевої підсистеми, а безпосередній доступ до віртуальної машини передбачається за звичайними мережевими інтерфейсами. Тому, для побудові кіберполігону на базі технологій Proxmox VE чи аналогічній, може бути актуальним розгортання програмного маршрутизатору, наприклад, на базі дистрибутивів: pfSense (https://www.pfsense.org/), OPNsense (https://opnsense.org/), IPFire (https://www.ipfire.org/), чи ін. Завдяки такому рішенню можна в лічені години розгорнути складну віртуальну мережу для моделювання інфраструктури підприємства й поруч із цим отримати зручний доступ до віртуальних серверів системи.

Висновки. Пропонується застосування систем віртуалізації для тестування та налагодження безпеки серверних систем на моделі серверної інфраструктури підприємства. Особливу увагу у формуванні відповідних рішень слід надавати конфігуруванню віртуальної інфраструктури мережі.

Список використаної літератури:

1. Алексієв В. О. Особливості розгортання сучасного веб-сайту / В. О. Алексієв, О. Д. Єрещенко, О. А. Скороход // Комп'ютерні технології і мехатроніка : зб. наук. пр. за матеріалами II міжнар. наук.-практ. конф. – Харків : ХНАДУ, 2020. – С. 298–301.

2. Алексієв В. О. Визначення методів та засобів для уніфікації процесу розробки веб-ресурсів малого підприємства / В. О. Алексієв, В. М. Горяінов // Матеріали VI міжнародної науково-технічної Інтернет-конференції "Автомобіль і електроніка. сучасні технології", 19-20 листопада 2018 р. – Х.: ХНАДУ. – 2018. – С. 48-50.