ПРОБЛЕМИ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ВІД ПОСЯГАНЬ ЗЛОВМИСНИКІВ

Лаврівська О. З. курсант; Грицюк Ю. І. д.т.н., проф.
Львівський ДУ БЖД, м. Львів, Україна

Швидкий розвиток телекомунікаційної галузі привів до того, що електронна пошта стала звичайним явищем, позаяк вирішила проблему ділового і особистого листування як у просторі, так і часі. Найбільш відчутною проблемою телекомунікаційних мереж та інформаційних технологій вважається інформаційна безпека [1]. Можна застосувати найдосконаліші засоби аутентифікації та криптографії, відгородитися потужним міжмережевим екраном, але незначна прогалина у відповідальній програмі здатна звести нанівець всі зусилля, надавши кваліфікованому зловмиснику можливість її використовувати у своїх намірах і врешті-решт отримати несанкціоновані права доступу [2].

Одним з методів, що дає змогу мінімізувати ризик вторгнення, називається *Honeypot* (від англ. — *горщик з медом*). Фактично *Honeypot* («пастка») — ресурс, який є приманкою для зловмисників [2]. Його завдання — піддатися атаці зловмисника або несанкціонованому дослідженню мережі, що згодом дасть змогу системному адміністратору вивчити стратегію зловмисника і визначити перелік засобів, за допомогою яких він зможе завдати удари по реально наявних об'єктах інформаційної системи. Реалізація *Honeypot* як пастки для зловмисників — не принципова: це може бути як спеціально виділений сервер, так і один з мережевих серверів, завдання якого — привернути увагу зловмисників [1].

Як правило, відомі засоби захисту мережевої інфраструктури призначені вирішувати строго певні функції [1]. Наприклад, міжмережевий екран розмежовує доступ з однієї мережі в іншу на різних рівнях, сервіс *SSH* призначений для шифрованого доступу до ресурсів операційної системи і т. д. Приманка *Honeypot* має велику перевагу над екранами і різними сервісами. Насамперед, це збирання необхідної інформації, що часто містить цінні відомості. Розкручування та експлуатація «живця», тобто зловмисника, не представляють особливих труднощів. Також засоби *Honeypot*, як правило, не вимогливі до надмірних системних ресурсів, якими обмежені більшість державних локальних мереж.

У приманці *Honeypot* назбирується інформації не так вже й багато, але вона представляє велику цінність для системного адміністратора мережі, адже саме такі відомості розкривають суть спроби її зламування, сканування або дослідження. Адміністратор мережі може провести аналіз атак і намірів зловмисника, побудувати статистику методів зламування системи, які використовуються хакерами, а також визначити наявність будь-яких нових рішень, що застосовуються зловмисниками. Необдумано було б під-

ставляти під удар реальну ділянку мережевої інфраструктури — адже на основі інформації від *Honeypot* можна оперативно внести корективи до конфігурації, наприклад, *production*-сервера.

Особливої уваги вимагає місце інсталяції та подальша експлуатація приманки *Honeypot* [2]. Як правило, весь комплекс заходів зводиться до «встановлення та очікування». Найбільш поширений випадок з виділеним сервером, який знаходиться під контролем фахівців. Перевага *Honeypot* в тому, що копію програмного забезпечення можна зробити на морально застарілому сервері, який не справляється з типовими обчислювальними завданнями електронного бізнесу.

Для того, щоб з'ясувати цінність пасток, розглянемо інформаційну модель безпеки Брюса Шнейера [1], яка бере до уваги три рівні: запобігання, виявлення, відповідь. *Honeypot*-пастки можуть бути задіяні на всіх трьох рівнях. Наприклад, на рівні запобігання вони застосовуються при уповільненні або повній зупинці автоматичних вторгнень. Пастки можна використовувати для виявлення неавторизованої активності, коли традиційні рішення з області безпеки здатні згенерувати величезний обсяг журнальних записів, тоді як всього декілька з них відображують реальні спроби проникнення або дослідження. Окрім цього, не всі сучасні інформаційні технології володіють інтелектуальними здібностями і не завжди можуть ідентифікувати досі не знайомі атаки. Приманка Honeypot з успіхом вирішує такі проблеми, позаяк через малий обсяг корисної інформації, що генерується, можна упевнитися в тому, що має місце атака або дослідження.

Описані вище переваги можуть викликати у недосвідченого читача ілюзію, ніби *Honeypot* — ідеальний засіб для забезпечення максимальної безпеки. Шкода, але приманка Honeypot може тільки слугувати доповненням до наявного комплексу засобів захисту мережевої інфраструктури. Насамперед конкретні пастки мають вузьку спрямованість, також існує ймовірність виявлення *Honeypot* та небезпеки повного його зламування. Ця приманка потенційно не здатна охопити всі проблеми інформаційної безпеки, тому доводиться або досліджувати рівень безпеки окремо взятого фрагмента інфраструктури мережі, або застосовувати декілька приманок.

Окрім практичного застосування приманки *Honeypot* не менш важливий інший бік питання — дослідницький напрямок. Одна з найбільш актуальних проблем фахівців з інформаційної безпеки полягає у відсутності достовірної інформації про цей напрям діяльності. Адже за допомогою декількох машин з різним програмним забезпеченням можна значно більше дізнатися про дії хакера, ніж при використанні однієї пастки.

Література

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. — К. : Вид. група BHV, 2009. — 608 с.

2. Комплексна система захисту інформації. [Електронний ресурс]. — Доступний з http://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації.