ОГЛЯДИ. ПОЛЕМІКА. ОБМІН ДОСВІДОМ

УДК 004.056:061.68

ВИКОРИСТАННЯ ПРИМАНОК ДЛЯ ЗАХИСТУ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ВІД ПОСЯГАНЬ ЗЛОВМИСНИКІВ

Лаврівська О. З., Грицюк Ю. І., д.т.н., професор
Львівський державний університет безпеки життєдіяльності, Львів, Україна

USING TRAPS TO PROTECT NETWORK INFRASTRUCTURE FROM INTRUDERS' ATTACKS

Lavrivska O.Z., Grycyuk Yu.I., Doctor of Science (Technics), Professor
Lviv State University of Life Safety, Lviv, Ukraine

Проблеми захисту мережевої інфраструктури. Швидкий розвиток телекомунікаційної галузі привів до того, що електронна пошта стала звичайним явищем, позаяк вирішила проблему ділового і особистого листування як з точки зору часу, так і відстаней. Паралельно з цим користувачі пошти відчули і негативні аспекти прогресу, наприклад, небажана поява спаму[1]. Проте, найбільш відчутною проблемою телекомунікаційних мереж та інформаційних технологій можна вважати інформаційну безпеку [1]. Для її забезпечення придатні всі засоби, часто некоректні чи навіть несанкціоновані. Здавалося б можна застосувати найдосконаліші засоби аутентифікації та криптографії, відгородитися потужним міжмережевим екраном, але незначна помилка 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].

Достатньо довго в принципі протистояння «атака – захист» використовувалася своєрідна покрокова стратегія інформаційної безпеки: зловмисник скористався одним вразливим місцем — його з часом захистили. Тоді він знайшов наступне — його знову захистили і т.д. Нагадує це гру в шахи, де партія здатна тривати скільки завгодно. Зрозуміло, за цей час навіть невелика компанія може зазнати колосальних збитків, позаяк у хакера[2] знайдеться завжди можливість адекватно відреагувати на захисні заходи, якими б вони не були досконалими [7].

[1] Спам (англ. *spam*) — масове розсилання кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її отримувати. Термін «спам» стосується рекламних електронних листів. Також вважаються спамом освідчення в коханні на електронну пошту, в чатах, соціальних мережах і т.п.

[2] Хакер (англ. *hacker*, від to *hack* — рубати, шматувати) — надзвичайно кваліфікований IT-фахівець, людина, яка розуміє найособливіші моменти роботи комп'ютерних систем. Хакери з'явилися в той же час, що і мережа Інтернет, тобто в 1960 роках

Наприклад, в мережі Інтернет ще в 2010 році появилася публікація [6], в якій сказано, що двом хакерам вдалося зламати *iPhone* останньої на той час версії за 20 секунд. Атака була проведена на щорічному конкурсі *Pwn2Own*, який проводився в рамках конференції *CanSecWest* 2010. Перед хакерами було поставлено завдання якнайшвидше зчитати з *iPhone* всі СМС-повідомлення. З завданням найшвидше впоралися Вінченцо Йоццо і Ральф-Філіп Вайнманн. Вони направили *iPhone* на створений ними сайт, за допомогою якого, скориставшись невідомою раніше вразливістю пристрою, викрали базу СМС. За свою роботу хакери отримали 15 тисяч доларів, а також зламаний ними телефон. Переможці, один з яких був співробітником Університету Люксембургу, а інший працює в комп'ютерній фірмі Zymanics, розробляли протягом двох тижнів експлойт, що використовує уразливість iPhone. Вайнманн заявив, що крім СМС вони могли б викрасти список контактів, повідомлення електронної пошти, фотографії та музичні файли, однак це не входило в завдання організаторів конкурсу. У рамках конкурсу також були зламані браузери *Internet Explorer* 8, *Safari* і *Firefox*. За умовами організаторів атаки мали здійснюватися на останні версії програмного забезпечення зі встановленим захистом від усіх відомих вразливостей. За зламування браузерів були вручені призи в розмірі 10 тисяч доларів. Конкурс *Pwn2Own* проводив за кошти компанії *TippingPoint*, яка виробляє засоби захисту від комп'ютерних вторгнень. За традицією організатори конкурсу надають інформацію розробникам програмного забезпечення про використану для зламування його уразливість і роблять їх надбанням громадськості після впровадження випуску відповідних оновлень.

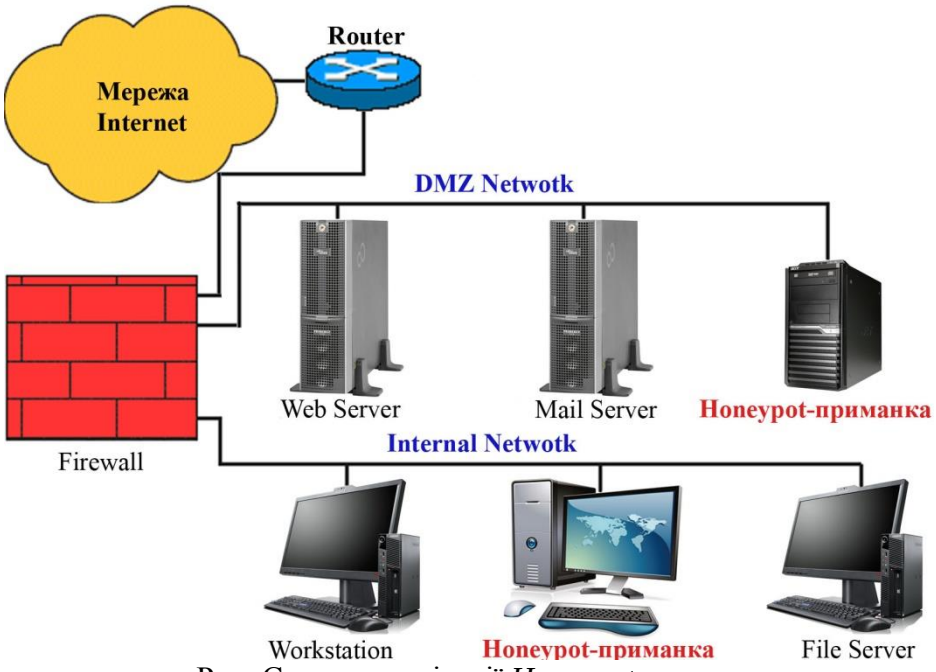

Рис. Схема організації *Honeypot*-пасток

Honeypot — нова технологія захисту мережевої інфраструктури. Часто потенційно потерпіла сторона, щоб мінімізувати ризик вторгнення зловмисників у мережеву інфраструктуру, зобов'язана робити відповідні дії на випередження. Одним з методів, що дає змогу здійснити цю ідею, називається Honeypot (від англ. — горщик з медом) [8]. Фактично *Honeypot* («пастка») — ресурс, який є приманкою для зловмисників [3, 5]. Завдання *Honeypot* — піддатися атаці зловмисника або несанкціонованому дослідженню, що згодом дасть змогу системному адміністратору вивчити його стратегію і визначити перелік засобів, за допомогою яких він зможе завдати удари по реально наявних об'єктах інформаційної безпеки. Реалізація *Honeypot* як пастки для зловмисників — не принципова (рис.), — це може бути як спеціально виділений сервер, так і один з мережевих серверів, завдання якого — привернути увагу зловмисників [4].

Технологія захисту мережевої інфраструктури *Honeypot* кардинально відрізняється від всіх розробок у сфері інформаційної безпеки [3]. Як правило, всі відомі програмні продукти покликані вирішувати строго певну функцію (неважливо, то апаратне чи програмне забезпечення). Наприклад, міжмережевий екран вирішує завдання розмежування доступу з однієї мережі в іншу на різних рівнях, сервіс *SSH*[3] призначений для шифрованого доступу до ресурсів операційної системи і т.д. Приманка Honeypot має велику перевагу над екранами і різними сервісами [8]. 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.

Величезна кількість програмних продуктів, які існують на ринку інформаційної безпеки, має розвинені вбудовані механізми збирання та аналізу інформації (в основному на рівні журналів), що стосуються безпеки. Мережевий адміністратор здатний відстежити події в хронологічному порядку і дізнатися, що відбувалося на певній ділянці мережевої інфраструктури в будь-який момент часу [5]. Хоча 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.

Оскільки приманка *Honeypot* початково призначалася для відстежування атак і досліджень намірів зловмисників, то вважається, що практично вся знята з цієї пастки інформація відображає саме їхні дії. На основі отриманих даних адміністратор мережі може провести їх аналіз, побудувати статистику методів зламування системи, які використовуються хакера-

[3] *SSH* (англ. *Secure SHell* — «безпечна оболонка») – мережевий протокол рівня додатків, який дає змогу проводити віддалене управління операційною системою і здійснювати тунелювання *TCP*-з'єднань (наприклад, для передачі файлів).

ми, а також визначити наявність будь-яких нових рішень, що застосовуються зловмисниками [7]. Необдумано було б підставляти під удар реальну ділянку мережевої інфраструктури — адже на основі інформації від приманки *Honeypot* можна оперативно внести корективи до конфігурації, наприклад, *production*-сервера.

Особливої уваги вимагає місце інсталяції та подальша експлуатація приманки *Honeypot* [5]. Як правило, весь комплекс заходів зводиться до «встановлення та очікування». Найбільш поширений випадок з виділеним сервером, який знаходиться під контролем фахівців. На сьогодні є безліч програм-підробок, які справляють враження сьогодення, але не є такими, позаяк їх основне завдання — протоколювати весь обмін даними. 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, наприклад, інформаційну модель безпеки Брюса Шнейера (*Bruce Schneier)*, яка бере до уваги три рівні: запобігання, виявлення, відповідь [1]. *Honeypot*-пастки можуть бути задіяні на всіх трьох рівнях [3, 5]. 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 легко упевнитися в тому, що має місце атака чи дослідження. Пастки використовуються і для реакції спроби зловмисника вторгнутися в мережеву інфраструктуру [8]. Якщо зловмисник проник у мережу і одна з атакованих систем виявилася пасткою, корисна інформація, отримана від цієї пастки, використовується для відповіді на атаку.

Описані вище переваги можуть викликати у ламера[4] ілюзію, ніби *Honeypot* — ідеальний засіб для забезпечення максимальної безпеки. Шкода, але через деякі недоліки приманка *Honeypot* може тільки слугувати доповненням до наявного комплексу засобів захисту мережевої інфраструктури [5]. Насамперед потрібно відзначити вузьку спрямованість конкретної пастки, також існує ймовірність виявлення *Honeypot* та небезпеки повного її знищення. Ця приманка потенційно не здатна охопити всі проблеми ін-

[4] Ламер — на комп'ютерному сленгу так називають людину, яка погано володіє комп'ютером, нездатного або принципово не бажає добре освоїти роботу за комп'ютером. Для програмістів — образливе слово. Часто цей термін використовується для протиставлення понять «хакер» чи «комп'ютерний гуру». Замість слова «ламер» часто вживають слово «чайник» в значенні «недосвідчена людина».

формаційної безпеки, тому доводиться або досліджувати рівень безпеки окремо взятого фрагмента інфраструктури мережі, або застосовувати декілька приманок (див. рис.).

Також не можна вилучити ризик усвідомлення зловмисниками того, що перед ними не реальний обсяг інформації, а тільки підставна пастка [3]. Найчастіше це відбувається через неправильні або недостатньо ретельні налаштування пастки, тобто здебільшого винен людський чинник. Наприклад, приманки Honeypot спочатку замасковували під сервер доменних імен (*DNS*), що працює під управлінням ОС *Sun Solaris*. Якщо сервер з будь-яких причин почав працювати під ОС *Linux*, то можна не сумніватися — зловмисник запідозрить пастку. Ще одна типова проблема — активність роботи сервера: якщо це не реальний комп'ютер, то найчастіше він не проявлятиме жодної активності (знаходячись в пасивному режимі очікування зламування) і не генерували постійно мережевий трафік, що відразу ж виявить зловмисник.

Окрім практичного застосування приманки *Honeypot*, описаної вище, не менш важливий інший бік питання — дослідницький напрямок [8]. Шкода, проте 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.

Висновки: 1) З'ясовано, що приманка *Honeypot* — гнучка інформаційна технологія, яку можна застосовувати у багатьох ситуаціях. Як засіб забезпечення безпеки, *Honeypot*-пастки мають здатність ефективно працювати в мережі інфраструктури, збираючи невелику кількість даних, проте значна їх частина має чимале значення для власників мережі. Також *Honeypot*-приманки можуть ефективно працювати в інтенсивному середовищі, не вимагаючи при цьому великих витрат на їх розгортання та експлуатацію.

2. Виявлено, що основними недоліками *Honeypot*-пастки є те, що вона значно звужує область бачення проблем. Якщо приманка Honeypot не атакована, то вона не має ніякого значення. Деякі *Honeypot*-пастки піддаються різким методам розкриття зловмисниками і можуть бути виявлені або, що найгірше, використані для проникнення в інші системи.

3. Встановлено, що приманки *Honeypot* можуть застосовуватися як у виробничій сфері, виконуючи функції попередження, виявлення та реакції на дії зловмисника, так і бути частиною дослідження щодо виявленню нових методів, засобів і мотивацій зловмисників.

Література

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

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р., № 80/94, редакція від 30.04.2009 р. [Електронний ресурс]. — Режим доступа: http://zakon4.rada.gov.ua/laws/show/80/94-вр

3. Михеев Д. Приманка для мух: технологии Honeypot / Д. Михеев. [Электронный ресурс]. — Режим доступа: http://www.itsec.ru/articles2/Oborandteh/priman ka_dlya_muh

4. Обнаружение и противодействие honeypots: системные вопросы [Электронный ресурс]. — Режим доступа: http://www.nestor.minsk.by/sr/2005/05/sr50516.html

5. Патий Е. Honeypot: приманка для злоумышленника / Е. Патий. [Электронный ресурс]. — Доступный с http://citcity.ru/15560/

6. Хакеры взломали iPhone за 20 секунд [Электронный ресурс]. — Режим доступа: http://www.segodnya.ua/science/khakery-vzlomali-iphone-za-20-cekund.html

7. Хто такі хакери і що вони собою представляють [Електронний ресурс]. — Режим доступа: http://http://hakyr.blog.net.ua/

8. Honeypot — приманка для нарушителя [Электронный ресурс]. — Режим доступа: http://cybern.ru/honeypot.html

References

1. Haivoronskyi M. V., Novikov O. M. (2009) Bezpeka informatsiino-komunikatsiinykh system [Security Information and Communication Systems]. Kyiv, BHV Publ., 608 p.

2. Zakon Ukrainy “Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh” [The Law of Ukraine “Data Protection in the information and telecommunication systems”]. Available at: http://zakon4.rada.gov.ua/laws/show/80/94-вр (Accessed 01 Dec 2013)

3. Mikheyev D. Bait for the flies: Honeypot technology. Available at: http://www.itsec.ru/articles2/Oborandteh/priman ka_dlya_muh (Accessed 01 Dec 2013)

4. Detection and counteraction honeypots: System Aspect. Available at: http://www.nestor.minsk.by/sr/2005/05/sr50516.html (Accessed 01 Dec 2013)

5. Patyi E. Honeypot: bait for attackers. Available at: http://citcity.ru/15560/ (Accessed 01 Dec 2013)

6. IPhone hackers broke into the 20 seconds. Available at: http://www.segodnya.ua /science/khakery-vzlomali-iphone-za-20-cekund.html (Accessed 01 Dec 2013)

7. Who are hackers and what they represent. Available at: http://http://hakyr.blog.net.ua/ (Accessed 01 Dec 2013)

8. Honeypot - bait for the intruder. Available at: http://cybern.ru/honeypot.html (Accessed 01 Dec 2013)

Лаврівська О. З., Грицюк Ю. І. ***Використання приманок для захисту мережевої інфраструктури від посягань зловмисників.*** *Розглянуто особливості використання приманок для захисту мережевої інфраструктури від посягань зловмисників, які стосуються ризиків несанкціонованого їх вторгнення в мережу: атаки на мережу, несанкціоноване її дослідження і т.д. З'ясовано, що приманка Honeypot — гнучка інформаційна технологія, яку можна застосувати для запобігання атак, їх виявлення та відповіді на них. Як засіб забезпечення безпеки, Honeypot-пастки мають здатність ефективно працювати в мережі інфраструктури, збираючи невелику кількість даних, проте значна їх частина має велике значення для власників мережі.*

Ключові слова: *приманка Honeypot, інфраструктура мережі, засоби захисту інформації, інформаційні атаки, інформаційні загрози.*

Лаврівская О. З., Грыцюк Ю. И. ***Использование приманок для защиты сетевой инфраструктуры от посягательств злоумышленников.*** *Рассмотрены особенности использования приманок для защиты сетевой инфраструктуры от посягательств злоумышленников, касающиеся рисков несанкционированного их вторжения в сеть: атаки на сеть, несанкционированное ее исследование и т.д. Выяснено, что приманка Honeypot — гибкая информационная технология, которую можно применить для пре-*

дотвращения атак, их выявления и ответа на них. Как средство обеспечения безопасности, Honeypot-ловушки имеют способность эффективно работать в сети инфраструктуры, собирая небольшое количество данных, однако значительная их часть имеет большое значение для владельцев сети.

Ключевые слова: *приманка Honeypot, инфраструктура сети, средства защиты информации, информационные атаки, информационные угрозы.*

Lavrivska O. Z., Grycyuk Yu. I. ***Using traps to protect network infrastructure from intruders' attacks.*** *The article deals with the peculiarities of using traps to protect network infrastructure from intruders' attacks concerning the risks of unauthorized intrusion to a network: attacks on a network, its unauthorized research, etc. It has been clarified that Honeypot trap is flexible information technology, which can be applied to prevent attacks, their detection and answer to them. As a means of protection Honeypot-traps have ability to work effectively in the infrastructure network collecting small amount of data. However, they are of considerable importance for the owners of network.*

Keywords: *Honeypot trap, network infrastructure, means of information protection, information attacks, information threats.*