УДК 004.051
DOI: 10.31673/2409-7292.2020.025968

Гапоненко О. І., Марченко В.В., Гайдур Г.І.

ПЕРЕВАГИ ТА НЕДОЛІКИ HONEYPOT – ПРИМАНКИ ДЛЯ ХАКЕРІВ

Розглянуто історію виникнення Honeypot та проаналізовано переваги і недоліки використання «Приманки для хакерів», як інструмент для статистичного моделювання, аналізу дій, виявлення нападів або дослідження поведінки зловмисників.

Ключові слова: Honeypot, спам, DoS, кіберінциденти, міжмережевий екран, зловмисник.

Вступ

З кожним днем загрози для мережі збільшуються з великим процентом, тому для безпеки наших даних потрібно знаходити нові технології. Honeypot є чудовим інструментом для доповнення системи захисту від кіберінцидентів.

Для розуміння, що таке Honeypot потрібно розглянути, як саме було винайдено цю технологію, її подальший розвиток. Далі потрібно розглянути саму роботу Honeypot, та його види і їх принципи роботи.

Історична довідка

Прототип Honeypot було ще зроблено в 1986 році системним адміністраторм Кліффордом Столлом, він помітив дев'ять секунд неоплачуваного комп'ютерного часу в Національній лабораторії ім. Лоуренса в Берклі. Коли його попросили вирішити цю проблему, Столл в результаті прийшов до висновку, що хакер незаконно отримав доступ до своєї мережі, використовуючи вразливість. Столл вирішив, що він влаштує пастку для хакера. Він зібрав 50 комп'ютерних терміналів зі свого офісу, підключив термінали до телефонних ліній офісу і чекав. Зрештою, хакер набрав номер і Столл простежив дзвінок в компанію по імені Tymnet. За допомогою Tymnet вони простежили і впізнали хакера, як новобранця КГБ Маркуса Гесса. Цей випадок було описано в книзі Кліффорда Столла «The Cuckoo's Egg». Через десять років, у 2000 р. Honeypot почав поширюватися як система для приманок[3].

Технологія Honeypot та її різновидності

Більшість технологій безпеки розроблені для вирішення конкретних проблем. Наприклад брандмауер запобігає атакам, керуючи потоком руху трафіка, що проходить через нього та антивірусне програмне забезпечення визначає, очищає та захищає комп’ютери від зловмисного програмного забезпечення. Цілі Honeypot визначається намірами тих, хто розробляє або розгортає його. Honeypot може, допомогти зупинити або виявити мережеві атаки – завданням, яких спільно використовуються між брандмауером або мережею система виявлення вторгнень. З іншого боку, Honeypot також можуть бути розроблені для більш творчих завдань, таких як відволікання атак від критичних ресурсів та заохочення кіберзлочинця залишатися в системі досить довго, щоб забезпечити збір обширної інформації про діяльність зловмисника. Зібрана інформація згодом буде використана для захисту мережі від подібних атак. Завдяки гнучкості та безлічі різних застосувань Honeypot, тому така характеристика дуже широка за обсягом.

«Honeypot – це ресурс інформаційної системи, цінність якої полягає у несанкціонованому чи незаконному використанні цього ресурсу». Таким ресурсом може бути маршрутизатор, принтер, виконання скриптового сценарію, на яких працює емульована служба, яка вбудована систему з – або емуляцією відомих вразливостей, або будь-яким типом цифрової техніки. Вони спеціально відрізняються від діючої системи тим, що вони не надають виробничих послуг, а тому вони не загружають систему. Для цього будь-яка діяльність з Honeypot або взаємодія з ним слід вважати несанкціонованим та підозрілими[4].

Honeypot працює, обдурюючи зловмисників, вважаючи, що це законна система; вони атакують систему не знаючи, що за ними таємно спостерігають.

Коли зловмисник намагається скомпрометувати пастку то буде зібрана інформація, що стосується нападу, наприклад IP-адреса зловмисника. Ця діяльність, що була здійснена

зловмисником надає цінну інформацію та аналіз прийому атаки, це дозволяє системним адміністраторам "відстежувати" де саме джерело атаки, якщо потрібно.

Основна перевага використання технології Honeypot полягає в області виявлення. Завдяки своїй спрощеній природі, він легко вирішує проблеми з якими стикаються IDS. За допомогою Honeypots ми можемо значно зменшити проблеми помилкових позитивних результатів та помилкових негативів. На відміну від IDS, весь трафік, який отримують Honeypot, вважається нападом. Також системи IDS зазвичай залежать від верісії яку купили у вендорів, а в разі атаки «нульового дня» системи IDS не видають сповіщення. Інша проблема IDS полягає в тому, що вони працюють у робочому середовищі, їм доводиться стикатися з великою кількістю трафіку, що проходить через них, і у відповідь вони створюють великі набори журналів, які важко проаналізувати.

Мережеві адміністратори це питання вирішується Honeypot, оскільки він не має робочої цінності. Все, що отримують Honeypot, є нападом і воно не включає жодних даних, пов’язаних з робочим трафіком. Також у разі нападу Honeypot можна витягнути в автономному режимі для проведення детальних розслідувань та криміналістики, що іноді складно, якщо не неможливо з робочими системами. Комерційні організації отримують найбільш пряму вигоду від виробничих Honeypot.

Брандмауери, як правило, розгорнуті для захисту середовища від будь-якого несанкціонованого доступу. Однак Honeypot розроблені для того, щоб обманути кіберзлочинців на проведенні атаки. Після того, як порушник зайде в систему, дослідник безпеки може знати, як вони працюють. Використовуючи цю інформацію, аналітик безпеки в компанії може знати, які системи та порти кіберзлочинців найбільше цікавлять. Також брандмауери проводять журнал діяльності всіх систем в організації, тому у випадку події стає важко переглядати всі журнали, щоб знайти певну подію. Як і IDS, журнали брандмауера також містять події, пов'язані з виробничими системами. Однак у випадку з Honeypot, журнали пов'язані лише з проблемами та атаками. Отже, якщо журнал брандмауера містить 1000 записів усіх систем у мережі, журнал Honeypot містить лише 5-10 записів. Кожен з них важливий для використання в системній безпекці[5].

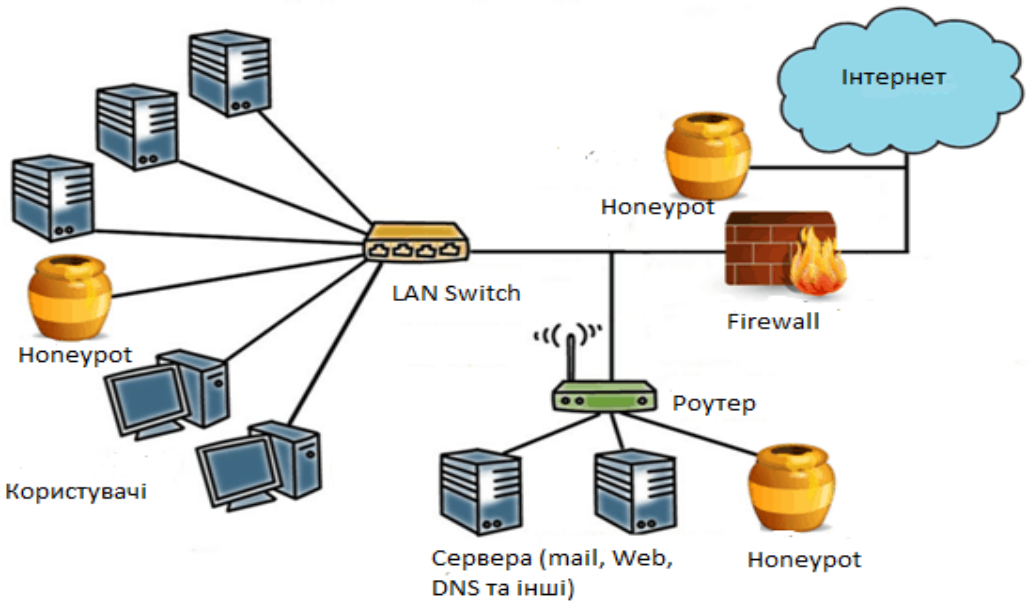

Рис. 1. Приклад розміщення Honeypot в мережі

Існують два основних види Honeypot:

1). Дослідницький Honeypot: Цей тип пастки використовується розробниками, системними адміністраторами та менеджерами blue team, що працюють в таких установах, як університети, коледжі, школи та інші пов'язані асоціації.

2). Виробничий Honeypot: Цей використовується приватними та державними установами, компаніями та корпораціями для дослідження поведінки та піймання кіберзлочинців, які прагнуть атакувати мережі в Інтернеті.

Honeypot стратегічно побудований для того, щоб обманути кіберзлочинця, вважаючи, що він знайшов спосіб змінити права та викрасти авторизацію. Коли спрацьовує пастка, на центральний сервер обману надсилається тривога, яка бере до уваги постраждалого приманку та вектори атаки, які використовували кіберзлочинця.

Він розроблений свідомо з відомими експлойтами в системі, щоб заманити кіберзлочинця. Honeypot не може містити виробничі дані або брати участь у справжньому трафіку мережі. Це вказує на те, якщо в ньому з'являється активність то це спроба взлому або несанкціонованому доступу в мережу.

Приклади Honeypot:

Деякі системні інженери схильні класифікувати Honeypot на основі цільового програмного забезпечення, яке вони намагаються захистити або викрити. Тому перелік Honeypot може бути обширним в цій роботі розглянемо найпопулярніші його види :

Spam Honeypot: Також відомий як пастка для спаму, цей Honeypot створений спеціально для того, щоб ловити спамерів перш ніж вони потрапляють на законні скриньки електронної пошти.

Malware Honeypot: Цей тип Honeypot створений для імітації вразливих програм, API та систем з метою отримання атак зловмисних програм. Дані, які потім збираються, згодом будуть використані для розвідки зловмисного програмного забезпечення для створення ефективних детекторів злоякісних програм.

Database Honeypot: Бази даних є загальною ціллю веб-зловмисників і встановивши медовий бази даних, ви можете переглядати та вивчати різні методи атаки, такі як інжекція SQL, зловживання привілеями, експлуатація служб SQL та багато іншого.

Spider Honeypot: Цей тип Honeypot працює так, що створюючи фейкові веб-сторінки та посилання, доступні лише веб-сканерам, а не людям. Щойно сканер отримує доступ до Honeypot, його виявляють разом із заголовками для подальшого аналізу, як правило для допомоги у блокуванні шкідливих ботів та сканерів рекламної мережі[6].

Переваги та недоліки технології Honeypot

Розглянемо переваги та недоліки Honeypot та зробимо розбір кожного пункту ретельно:

Переваги Honeypot

Технології Honeypot надають кіберзахисникам такі переваги:

Збір змістовної інформації

Засоби Honeypot, з іншого боку, збирають невелику кількість даних, але те, що вони дійсно збирають має зазвичай високе значення. Замість того щоб реєструвати гігабайти даних кожен день, більшість Honeypot збирає кілька мегабайт даних в день або навіть менше. Але дані, які були зареєстровані найбільш ймовірно є скануванням, дослідженням або атакою – тобто інформацією, що має високе значення.

Honeypot може дати точну інформацію в швидкому і легкому для розуміння форматі. Це спрощує аналіз і зменшує час реакції. Наприклад, проект Honeynet група, що досліджує варіанти побудови Honeypot, збирає в середньому менше 1 мегабайта даних в день. Незважаючи на те, що це – дуже невелика кількість даних, вони містять перш за все зловмисну діяльність. Ці дані можуть бути використані для статистичного моделювання, аналізу дій, виявлення нападів або навіть дослідження зловмисників. Пояснюється це тим, що кошти Honeypot не мають ніякого промислового значення і зроблені спеціально для того, щоб "заманити" зловмисника, таким чином, будь-яке з'єднання, здійснене з Honeypot, з високою часткою ймовірності є дослідженням хоста або атакою.

Невимогливість до системних ресурсів

Honeypot фіксують і контролюють невелику діяльність. Більшість систем виявлення вторгнень зазнають труднощів, контролюючи мережі, які мають великі пропускні спроможності. Швидкість передачі даних і кількість трафіку є занадто великими для датчика, щоб він міг проаналізувати кожен пакет. В результаті трафік відкинутий, і потенційні атаки на систему були пропущені. Honeypot, розгорнутий на тій же самій мережі, не зіткнеться з цією проблемою. Honeypot тільки фіксує дії, спрямовані на нього самого, таким чином, система не "переповнюється" трафіком. Там де система виявлення вторгнень може зазнати невдач через брак ресурсів, Honeypot навряд чи буде мати цю проблему. Додатковим плюсом обмежених вимог засоби Honeypot - те, що не потрібно інвестувати велику кількість грошових ресурсів в апаратні засоби для Honeypot.

Простота установки, конфігурації та експлуатації

Простота є найбільш значущим перевагою технології Honeypot. Немає ніяких химерних алгоритмів для розгортання. Потрібно лише встановити даний засіб в організації і чекати результатів. Звичайно ж, існують різні додаткові рішення для Honeypot - такі як база сигнатурних атак, реакцій і так далі. Але все, що використовують Honeypot, оперують однією передумовою: якщо хтось з'єднується з Honeypot, то це вимагає перевірки. Тут використовується головний принцип: чим простіше рішення, тим воно надійніше. Підвищення складності незаперечно веде до можливих помилок конфігурації та роботи системи в цілому.

Необхідність використання Honeypot

Міжмережеві екрани, блокуючи дії зловмисників, стають жертвами їх власного успіху. Керівництво може почати ставити під сумнів повернення своїх грошових вкладень у безпеку, оскільки вони відчувають, що немає більше загрози: "Ми вкладали капітал і розгорнули міжмережевий екран, і ми ніколи не зазнали нападу. Чому ми потребуємо міжмережевий екран, якщо нас ніколи не атакували? " Причина по якій вони ніколи не були атаковані, - міжмережевий екран, який допомагає і зменшує ризик. Інвестиції в інші технології безпеки такі як сильна ідентифікація, шифрування, стоять перед тією ж самою проблемою. Навпаки, кошти Honeypot швидко і неодноразово демонструють своє значення. Кожен раз, коли вони піддаються нападу так чи інакше підтверджується наявність зловмисників, фіксуючи несанкціоновану діяльність.

Недоліки Honeypot

З урахуванням всіх оголошених переваг, можна припустити, що засіб Honeypot буде остаточним рішенням для здійснення безпеки. На жаль, це не так. Засоби Honeypot мають кілька недоліків. Саме через цих недоліків Honeypot не замінюють ніяких механізмів безпеки; вони тільки працюють і розширюють повну архітектуру безпеки:

Обмежена область бачення

Найбільший недолік Honeypot – вузька область бачення. Honeypot здійснюють моніторинг діяльності, яка спрямована проти самих зловмисників. Якщо дії атакуючого спрямовані на різні підсистеми мережі, то Honeypot НЕ буде виявляти дану діяльність, якщо вона не спрямована безпосередньо на Honeypot. Якщо зловмисник ідентифікував Honeypot, то він може спробувати обійти його і проникнути в організацію. Таким чином, дуже обмежена область бачення Honeypot може виключити події, які трапляються поза цією галуззю.

Можливість розкриття Honeypot

Інший недолік Honeypot – це можливість здійснювати розкриття Honeypot зловмисником. Можливість розкриття Honeypot зловмисником - це збір інформації, з використанням якої зловмисник може ідентифікувати істинну сутність Honeypot, тому що він має певні очікувані характеристики або особливості поведінки. Наприклад, Honeypot може імітувати роботу Web-сервера. Всякий раз, коли зловмисник з'єднується з цим певним типом Honeypot, Web-сервер відповідає, посилаючи загальне повідомлення про помилки, використовуючи стандартний HTML. Це точна відповідь, який ми очікували б для будь-

якого Web-сервера. Однак є орфографічна помилка в одній з команд HTML, такий як перевірка правопису довжини слова - "legnht". Ця орфографічна помилка тепер є особливістю для даного Honeypot, і будь-який зловмисник може швидко ідентифікувати даний Honeypot через цю помилку в імітації. Неправильно експлуатований Honeypot може також ідентифікувати себе. Існують різноманітні методи, щоб відрізнити справжню систему або сервіс від кошти Honeypot.

Ризик злому і атаки на вузли сторонніх організацій

Третя вада Honeypot - ризик. Під ризиком мається на увазі, що Honeypot, на який нападають, можна використати, щоб напасти або пошкодити іншим системам або організаціям.

Різні Honeypot мають різні рівні ризику. Деякі вводять дуже невеликий ризик, в той час як інші надають зловмисникові всі можливості, щоб піти в нові наступи. Чим простіше Honeypot, тим менше ризик. Наприклад, Honeypot, який просто імітує кілька сервісів, складно скомпрометувати і використовувати для атаки інших систем. Ризик є змінним залежно від того, як кожен будує і розгортає Honeypot. Через своїх недоліків, ресурси Honeypot не можуть замінити інші механізми безпеки, такі як міжмережеві екрани і системи виявлення вторгнень. Швидше, вони покращують захист, працюючи з існуючими механізмами безпеки [7,8].

Висновок

Таким чином, основною перевагою технології Honeypot є можливість виявлення зловмисного втручання у роботу системи у той момент, коли зловмисник не підозрює, що його відслідковують. На відміну від IDS, весь трафік, який отримують Honeypot, вважається нападом, що унеможливлює пропуск зловмисного втручання. У той же час, головний недолік Honeypot – вузька область бачення. Якщо дії атакуючого спрямовані не на Honeypot, а на окремі підсистеми мережі, то Honeypot не буде виявляти дану діяльність.

Перелік посилань

1. D. Dagon, C. Zou, and W. Lee. Modeling botnet propagation using time zones. In Proceedings of the 13th Network and Distributed System Security Symposium (NDSS'06), 2006.
2. Neil Daswani, Michael Stoppelman, the Google Click Quality, and Inc Security Teams, Google. The anatomy of Clickbot.A. In USENIX First Workshop on Hot Topics in Understanding Botnets (HotBots), 2007
3. HoneynetProject, "About the honeynet project," 2008. http://www.honeynet.org/about
4. Project Honeypot [Електронний ресурс] – Режим доступу: https://www.projectHoneypot.org/
5. Amit D. Lakhani. Deception Techniques Using Honeypots. Dr. Kenneth G. Paterson Information Security Group Royal Holloway, University of London UK – 75 с.
6. HONEYPOT SECURITY: The Government of the Hong Kong Special Administrative Region. 2008 – 13 с
7. Caleb Townsend. What is a Honeypot? https://www.uscybersecurity.net/Honeypot
8. Securitycode. Что такое Honeypot и от чего защищать виртуальные ИС? 2011 https://habr.com/ru/company/securitycode/blog/119821

Надійшла: 28.04.2020 Рецензент: д.т.н., професор Кожухівський А.Д.

.