УДК 004.56+004.77

А. В. Притула
Л. М. Куперштейн

ТЕХНОЛОГІЯ HONEYPOT ЯК АЛЬТЕНАТИВНИЙ ПІДХІД ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

Вінницький національний технічний університет

Анотація
Проаналізовано переваги та недоліки використання Honeypot. Розглянуто роль Honeypot в кібербезпеці.
Ключові слова: honeypot, кібербезпека, вразливість.
Abstract
The advantages and disadvantages of using Honeypot are analyzed. The role of Honeypot in cybersecurity is considered.
Keywords: honeypot, cyber security,vulnerability.

Вступ

Технологія Honeypot - ресурс безпеки, призначення якого полягає в тому, щоб стати дослідженим або зазнати нападу. Це означає, що незалежно від того, яку структуру має засіб Honeypot, мета полягає в тому, щоб даний ресурс був досліджений, атакований і використаний зловмисником. Не має значення, чи є ресурс імітованим сервісом або повноцінною операційною системою. Головне, що сенс функціонування ресурсу полягає в нападі на нього.

Виходячи з такого визначення, технологія Honeypot помітно відрізняється від поширених технологій забезпечення безпеки. Більшість технологій забезпечення безпеки, що використовуються сьогодні, було спроектовано для вирішення якоїсь однієї задачі. Наприклад, міжмережеві екрани контролюють вхідний і вихідний мережевий трафік і використовуються як засіб блокування несанкціонованої активності. Системи виявлення вторгнень визначають атаки, проводячи моніторинг мережі і системної активності.

Засоби Honeypot відрізняються від класичних засобів забезпечення безпеки, таких як міжмережеві екрани або системи виявлення вторгнень, тим, що вони не покликані вирішувати будь-яку конкретну задачу. Навпаки, Honeypot - гнучкий засіб, який може бути застосований в різних ситуаціях. Наприклад, засоби Honeypot дозволяють запобігати або виявляти атаки. По суті, Honeypot включає в себе деяку функціональність практично всіх засобів забезпечення безпеки.

Результати дослідження

На сьогоднішній день існують дуже багато різних засобів, які допомагають захистити або попередити атаки на інформаційні ресурси. Зазвичай такі рішення коштують дорого і не всі компанії можуть дозволити собі їх встановлення. Метою дослідження є виявлення переваг та недоліків такого засобу як Honeypot, а також виявлення можливих сценаріїв, в яких він може бути корисним. На відміну від таких механізмів, як міжмережеві екрани і системи виявлення вторгнень, технологія Honeypot не вирішує певні завдання. Honeypot - це інструмент, який вносить свій внесок в повну архітектуру безпеки. Значення засобів Honeypot і проблеми, які вони допомагають вирішувати, залежить від того, як ці засоби побудовано, розгорнуто і як вони використовуються. Засоби Honeypot мають певні переваги і недоліки.

Аналітики наділяють Honeypot такими перевагами [1]:

- збір змістовної інформації;
- невимогливість до системних ресурсів;
- простота встановлення, конфігурації та експлуатації.

Завдання більшості механізмів безпеки - це аналіз зібраних даних. Організації щодня збирають великі обсяги даних, включаючи файли протоколу міжмережевих екранів, системні файли реєстрації подій і попередження систем виявлення вторгнень. Через велику кількість даних процес отримання потрібної інформації є надзвичайно важким. Засоби Honeypot, з іншого боку, збирають дуже невелику кількість даних, але те, що вони 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.

В процесі функціонування механізмів безпеки необхідно контролювати параметри обмеження ресурсів для того, щоб не виникла проблема нестачі ресурсів. Брак ресурсів – це коли механізм безпеки більше не може продовжувати функціонувати, тому що його ресурси вичерпані. Більшість систем виявлення вторгнень зазнають труднощів, контролюючи мережі, які мають великі пропускні спроможності. Швидкість передачі даних і кількість трафіку є просто занадто великими для датчика, щоб проаналізувати кожен пакет. В результаті трафік пропущений, і потенційні загрози нападу пропущені. Honeypot, розгорнутий на тій же самій мережі, не зіткнеться з цією проблемою. Honeypot тільки фіксує дії, спрямовані на нього самого, отже, система не "переповнюється" трафіком. Таким чином, Honeypot може не тільки працювати в досить швидкісній мережі, але і при цьому бути розгорнутим при досить дешевому технічному забезпеченні.

Простота є найбільш значущим перевагою технології Honeypot. Немає ніяких алгоритмів для розгортання Honeypot. Потрібно лише встановити даний засіб в організації і чекати результатів.

Звичайно ж, існують різні додаткові рішення для Honeypot такі, як база сигнатур атак, реакцій тощо. 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.

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

Головними проблемами засобів Honeypot є [1, 2]:

- обмежена область бачення;
- можливість розкриття Honeypot;
- ризик злому Honeypot і атаки вузлів сторонніх організацій.

Найбільший недолік засобів Honeypot – вузька область бачення. Honeypot здійснюють моніторинг діяльності, яка спрямована проти них. Якщо дії атакуючого спрямовані на різні підсистеми мережі, то Honeypot не буде виявляти таку діяльність, якщо вона не спрямована безпосередньо на нього. 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 його покриттям.

Інший недолік засобів Honeypot – це можливість розкриття Honeypot зловмисником. Розкриття Honeypot зловмисником – це збір інформації, з використанням якої зловмисник може ідентифікувати істинну сутність Honeypot, тому що він має певні характеристики або особливості поведінки. Розкриття Honeypot може негативно вплинути і з наступного боку: зловмисник, ідентифікувавши Honeypot, починає з ним взаємодіяти і, таким чином, помилково призводить адміністраторів в готовність. Тим часом, зловмисник може зосередитися на реальних нападах.

Третя вада Honeypot – ризик. Під ризиком мається на увазі, що Honeypot, який піддається нападу, може використовуватися, щоб напасти або зашкодити іншим системам або організаціям. Різні Honeypot мають різні рівні ризику. Деякі мають 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.

Виходячи із значення Honeypot, їх переваг і недоліків, варто проаналізувати, яку роль вони відіграють в інформаційній безпеці. Існують дві категорії, залежно від поставлених завдань, які ставляться перед засобами Honeypot: виробничі і дослідницькі Honeypot. Залежно від категорії існує певна різниця в тому, яку мету ставлять Honeypot в забезпеченні інформаційної безпеки.

Виробничі Honeypot - системи, що допомагають знизити ризик в організації або середовищі. Вони мають певний вплив на забезпечення безпеки систем і мереж. Дані Honeypot можуть бути використані

для вирішення основних завдань забезпечення інформаційної безпеки [3, 4]: попередження, виявлення, протоколювання. Одна з найбільших проблем фахівців з безпеки - нестача інформації. Такі питання, як: хто є загрозою, навіщо вони атакують, яким чином, які кошти використовують, – часто залишаються без відповідей. Щоб захиститися від загрози, потрібно спочатку знати про неї. Традиційно, професіонали безпеки дізнавалися про зловмисників, вивчаючи які інструменти вони використовували. Коли система була скомпрометована, адміністратори часто знаходили сліди зловмисників, залишені ними на атакований системі.

Дослідницькі Honeypot мають велике значення, надаючи платформу для вивчення загроз. Один із найкращий способів дізнатися про зловмисників – спостерігати за ними, записуючи кожен їх крок, під час нападу або компрометації системи [5]. Замість того щоб тільки знаходити використані зловмисником засоби, є можливість бачити, як зловмисник досліджує систему і починає атаку .У загальному випадку, дослідні Honeypot не зменшують ризик для організації, але отримана інформація може бути застосована на реальних системах, наприклад, для поліпшення, попередження, виявлення загроз, можливостей протоколювання і зменшення часу, необхідного для реакції на реальні атаки.

Висновки

Отже, Honeypot – це нестандартний інструмент для кібербезпеки. Зазвичай такі засоби створені для захисту або попередження атак, а Honeypot навпаки, створений для того, щоб його атакували та досліджували зловмисники. Така концепція відкриває багато можливостей для фахівців інформаційної безпеки, адже набагато краще спостерігати за зловмисником в той момент, коли він виконує свої маніпуляції, а не постфактум. Звісно ця технологія не позбавлена недоліків, але при правильному використанні може надати більше інформації та попередити від більшої кількості загроз, аніж інші інструменти захисту.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. Honeypots: Tracking Hackers / Lance Spitzner // monograph. – 2003. – Addison Wesley., англ. – Monograph. : 452 p.
2. Deniz Akkay, Fabien Thalgott. Honeypots in Network Security. URL: http://www.diva-portal.org/smash/get/diva2:327476/fulltext01 (дата звернення: 04.03.2021)
3. A Review on Creation of Dynamic Virtual Honeypots Using Hadoop. URL: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=4771f0ac-4bd6-4f6f-a0a6-7cd795727c4e&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (дата звернення: 04.03.2021)
4. A. Barfar, S. Mohammadi. Honeypots: Intrusion deception. URL: https://www.researchgate.net/publication/228854989_Honeypots_Intrusion_deception (дата звернення: 06.03.2021)
5. O. Catakoglu, M. Balduzzi, D. Balzarotti. Attacks Landscape in the Dark Side of the Web. URL: http://www.madlab.it/papers/sac17_darknets.pdf (дата звернення: 06.03.2021)

Притула Андрій Вікторович – студент групи 2БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: andrik.pritula@gmail.com.

Куперштейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

Prytula Andrii V. – Student of Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, e-mail: andrik.pritula@gmail.com.

Kupershtein Leonid M. — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com