ПРИНЦИП ДІЇ ТЕХНОЛОГІЇ HONEYPOT ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Валерія Войтович, Марія Шабатура

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

An analysis of existing systems of virtual lures based on honeypot technology. The analysis showed the evolution of honeypot systems from Low-Interaction Honeypots to the most up-to-date Gen III Honeynets and pointed to the disadvantages of existing solutions. In addition, the classification of honeypot-systems has been carried out on a symbolic basis.

Keywords: virtual lure, honeypot technology, intrusion detection, honeynet, a hallmark classification principle.

Honeypot – це комп'ютерна система, яка створена для того, щоб заманювати кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. Еволюцію Honeypots можна побачити не озброєним оком, поглянувши на те, як ці системи використовуються разом із IDS для запобігання, виявлення та реагування на атаки. Дійсно, honeypots все частіше знаходить своє місце поряд з мережевими і хост-системами захисту від вторгнень.

Honeypots можуть запобігти атакам кількома способами. Перше – сповільнення або припинення автоматичних атак, таких як хробаки або авторучки [1]. Це атаки, які випадково сканують всю мережу, яка шукає вразливі системи. (Honeypots використовують різноманітні трюки TCP, щоб помістити зловмисника в "холдинг"). Другий шлях – запобігти людським атакам. Тут honeypots прагнуть зіткнутися з нападником, змушуючи його приділяти увагу діяльності, яка не завдає ні шкоди, ні втрати, надаючи організації час відповісти і блокувати атаку.

Виділяють два основних типи реалізацій: адаптовані і реальні. Іноді їх визначають як низько і високоінтерактівні.

Перші здатні емулювати взаємодію від імені певного сервісу, наприклад, прийняти з'єднання на tcp-порт 22, прийняти від атакуючого ім'я користувача і пароль і так далі, при цьому фіксуючи всі дії атакуючого.

Високоінтерактівні honeypot, засновані на застосуванні реальних ОС і реальних сервісів, трохи складніше в застосуванні. Фактично вони являють собою спеціально спроектовані мережеві сегменти, підключені до мереж загального користування. Мережевий трафік між honeypot і зовнішнім світом контролюється і фіксується, щоб повністю зберегти всі дії атакуючих, при цьому не допустивши шкоди для власної інфраструктури.

Типовими прикладами є honeyd і honeynet [2]. Honeyd дозволяє користувачам налаштовувати кілька віртуальних Honeypots з різними характеристиками і послугами на одній машині. Honeynet – це мережа, розміщена за реверсивним мереженим екраном, що фіксує усі вхідні і вихідні дані. Реверсивний файрвол обмежує об'єм шкідливого трафіку, що може покинути Honeynet-мережу. Ці дані зберігаються, фіксуються і контролюються. У середовищі Honeynet може бути розміщена будь-яка система, включаючи такі системи, які уже функціонують у виробничій мережі, яку покликана захищати Honeynet. Honeynet – це мережа, призначена бути атакованою і скомпрометованою для отримання відомостей про наявні та потенційні вразливості і загрози в мережі.

Сьогодні існує три основні архітектури Honeynet-мереж: I-ого покоління (Gen I Honeynets); II-ого покоління (Gen II Honeynets) та III-ого покоління (Gen III Honeynets).

Gen I Honeynets. Honeynet-мережі I-ого покоління обмежені в можливостях контролю та приборкування зловмисників, проте вони демонструють достатню ефективність у виявленні автоматизованих атак і атак початківців. Передусім Gen I Honeynets фокусуються на атаках відповідно можливостей. Такі мережі-приманки достатньо легко ідентифікуються.

Архітектура Honeynet-мереж I-ого покоління досить проста – ізольована мережа розміщується за пристроєм контролю доступу до мережі, найчастіше таким служить мережевий екран (рисунок 1, а). Мета такого розміщення – забезпечити неможливість атаки не honeypot-систем. Часто поряд з Honeynet-мережею знаходиться виробнича ІКС для адміністрування і накопичення зафіксованих даних. Також, можливим є розміщення інших контролюючих пристроїв (наприклад, маршрутизатора) для додаткового контролю [2]. Фіксація активності шляхом комбінації можливостей файрволу, IDS-сенсорів і системних логів забезпечує перехоплення інформації на таких чотирьох рівнях: активність в мережі, системна активність, активність програм та активність користувача. Gen II Honeynets. Технологія Gen II була розроблена в 2002 р. і направлена на усунення недоліків попередньої. Honeynet-мережі II-ого покоління простіші в розгортанні і складніші у виявленні [3]. Як описувалося вище, технологія Gen I виконувала контроль даних за допомогою мережевого екрану, що обмежував кількість можливих вихідних підключень. Незважаючи на свою відносну ефективність таке рішення є недостатньо гнучким і забезпечує легке «зняття зліпку». Honeynet-мережі II-ого покоління вирішують цю проблему шляхом модифікації загальної архітектури (рисунок. 1, б). Перша основна розбіжність – використання єдиного Honeynet-сенсора, що об’єднує функціонал файрвола та IDS. Друга основна відмінність – сама реалізація Honeynet-сенсора, що представляє собою пристрій другого рівня OSI (схожий на міст). Така реалізація значно ускладнює виявлення, так як відсутня маршрутизація пакетів, зменшення TTL і MAC-адреси пристроїв [4]. За рахунок описаних принципів Honeynet-мережа II-ого покоління може бути частиною основної виробничої мережі, а не ізольованою як в технології Gen I.

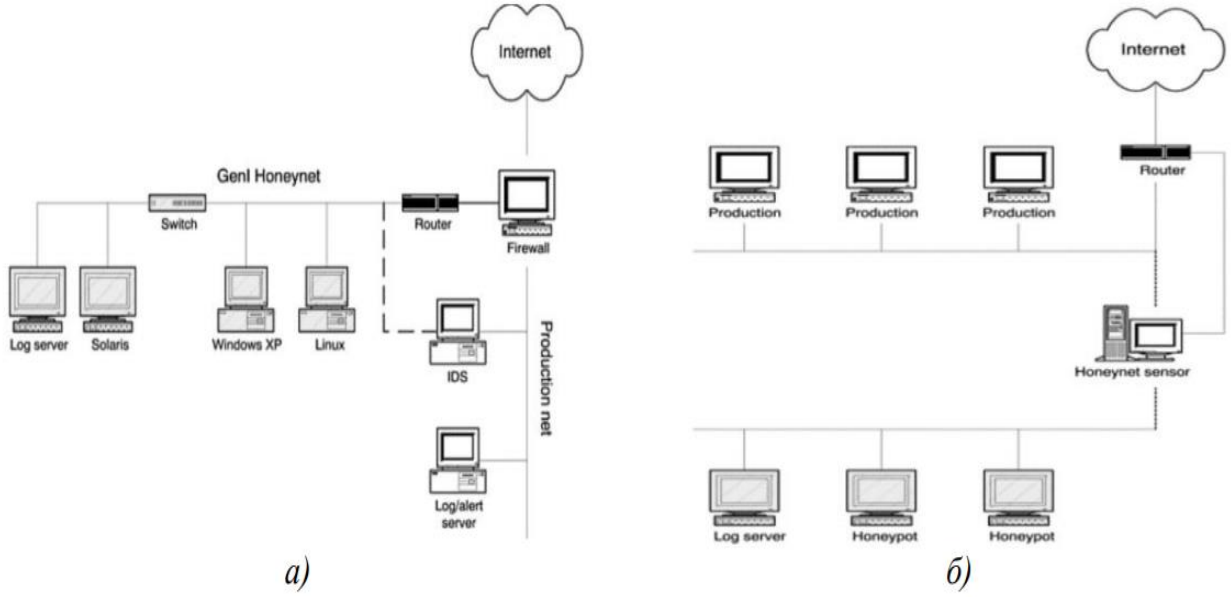

Рис. 1. Типова Honeynet-мережа: а) I-го покоління; б) II-го покоління Gen III Honeynets

Технологія Gen III реалізує подальше удосконалення і розширення можливостей контролю і аналізу даних. Модель аналізу даних базується на таки абстракціях: хости, процеси, мережеві потоки і файли (рисунок. 2). Такий підхід реалізується на основі використання системи Honeywall, розроблений фахівцями проекту Honeynet Project. Для контролю підключень і даних застосовується підхід IP Performance Measerment Working Group, що полягає в моніторингу потоків. У випадку використання Honeywall для цього застосовується система Argus [5]. Іншим удосконаленням є використання засобу пасивного зняття зліпку системи (passive fingerprinting), що ініціює TCP-підключення. Для об’єднання цих двох типів даних (активність в ІКС і процесів на хості) навколо суцільної картини концепції потоків мережі використовують додаткову зв’язуючу ланку. Для цього застосовують систему Sebek, що проводить моніторинг активності в мережі з перспективи

хоста [6]. У роботі виконано моделювання Honeynet Gen III у віртуальному середовищі UML, а праця містить варіант віртуалізації повноінтерактивних приманок.

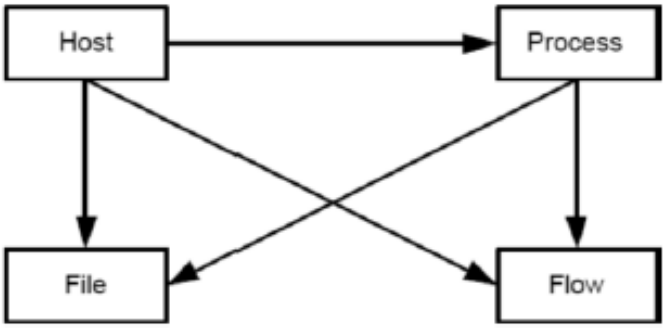

Рис. 2. Модель взаємозв'язків даних у системі Gen III

Висновок: подібно до всіх технологій, у honeypots є свої недоліки, найбільший з них – обмежена сфера їх перегляду. Honeypots захоплюють лише активність, спрямовану проти них, і буде пропускати напад на інші системи.

З цієї причини фахівці з безпеки не рекомендують ці системи, щоб замінити існуючі технології безпеки. Замість цього, вони бачать honeypots як додаткову технологію захисту від вторгнення.

Переваги, які приносять honeypots для захисту від вторгнень, важко ігнорувати, особливо зараз, коли починають розгортатися виробничі honeypot. З часом, коли розгортання розповсюдиться, honeypots можуть стати важливим компонентом операції безпеки на рівні підприємства.

Література

1. Мережні хробаки [Електронний ресурс]. Режим доступу: https://studfiles.net/preview/5206321/page:10/, вільний;
2. Spitzner, L. (2002), Honeypots: Tracking Hackers, 1st edition, Addison-Wesley, Boston, MA.
3. Know Your Enemy: Learning about Security Threats / Honeynet Project. — NY.: Addison-Wesley Professional, 2004. — 800 p.
4. Deal R. Router Firewall Security / R. Deal. — SF. : Cisco Press, 2004. — p. 912.
5. Argus and Infiniband [Електронний ресурс]: (ARGUS – Auditing Network Activity) // QoSient — Режим доступу: http://www.qosient.com/argus, вільний;
6. Balas E. Honeynet data analysis: A technique for correlating sebek and network data / E. Balas // Workshop on Information Assurance and Security US Military Academy, West Point, NY. — IEEE, 2004.