ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

БЕЛЬМА АНДРІЙ ВІКТОРОВИЧ

УДК 004.492

Методи розробки адаптивних контейнерних приманок (honeypots) для моніторингу кіберінцидентів

Спеціальність 125 «Кібербезпека»

Автореферат

дипломної роботи на здобуття освітньо-кваліфікаційного рівня «магістр»

Тернопіль — 2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат педагогічних наук, доцент
Кареліна Олена Володимирівна,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент, декан ФІС
Баран Ігор Олегович,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 23 грудня 2019 р. о 9 год. на засіданні Державної екзаменаційної комісії у Тернопільському національному технічному університеті імені Івана Пулюя за адресою:
46001, м. Тернопіль, вул. Руська, 56.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. На сьогодні до Інтернету під'єднано більше систем і пристроїв, ніж будь-коли раніше. Цією величезною кількістю пристроїв все частіше користуються люди з обмеженими технічними знаннями й ще меншою обізнаністю про загрози їх безпеки. З розширенням масштабів погано налаштованих заходів безпеки в системах, сучасний Інтернет стає для зловмисників ідеальним майданчиком з нескінченною кількістю пристроїв, які можуть бути зламані, експлуатовані та використані в безчесних цілях. Тому особливо актуальним є питання виявлення та протидії як старим, так і найновішим, ще невідомим типам та методам зламу, вірусам, шкідливому програмному забезпеченню та іншій зловмисній діяльності.

Вирішення цього складного завдання покладено на системи-приманки (англ. Honeypots) – привабливі для атаки об'єкти, що функціонують на основі спеціалізованого програмного забезпечення (ПЗ) та мають можливість реєструвати процедури зламу, виявляти та аналізувати мережні атаки. Серед науковців, які розв'зували окремі проблеми в цій області, можна назвати таких відомих вчених як С. Даулінг, М. Антонакакіс, І. Мокубе, М. Наврокі, Е. Васіломанолакіс, Т. Баррон, Н. Провос, П. Пісарчік та інші. Проте значна кількість проблем ефективного використання приманок, попри зусилля багатьох розробників, досі не вирішена. Зокрема, існуючі дослідження не приділяють достатньо уваги тому, як спонукати зловмисників взаємодіяти з приманками, натомість зациклюючись на самій взаємодії.

Мета і завдання дослідження. Метою дипломної роботи є дослідження та розроблення методів побудови контейнерної повно-інтерактивної мережі приманок з активним моніторингом, спрямованої на забезпечення стійкості до впливів зловмисника, прихованості й ізольованості механізмів збору та обробки інформації. Реалізація мети дослідження обумовила поставлення та розв'язання таких завдань:

- Аналіз методів проектування приманок та візуалізації їх даних засобами стеку ELK;
- Проектування адаптивної приманки для заохочення взаємодії з нею;
- Розроблення інтерактивної мережі приманок з використанням контейнерного середовища.

Об'єктом дослідження дипломної роботи є процес отримання та аналізу інформації з систем, що виконують роль приманок, з метою вивчення діяльності зловмисника під час зламу.

Предметом дослідження є методи та засоби організації систем збору та моніторингу інформації з приманок.

Методи дослідження. В процесі дослідження використано методи побудови обчислювальної мережі, контейнеризації, TCP/IP, Honeypot, Honeynet, візуалізація за допомогою стеку ELK. Також використовувались загальнонаукові методи пізнання: порівнювання, системний аналіз, моделювання.

Інформаційною основою дипломної роботи є праці закордонних вчених з питань розробки та ефективного використання приманок.

Наукова новизна роботи:

- Вперше розроблено повно-мережеву систему інтерактивних приманок з активною системою моніторингу як єдиний розгорнутий блок, який можна розмістити в Linux-системах.
- Вперше розглянуто адаптацію конструкції приманки для більш активного залучення атак.

Практичне значення дослідження полягає у можливості застосування розробленої системи в діяльності об'єктів критичних інфраструктур для активної протидії кіберзагрозам.

Апробація результатів дослідження. Окремі результати роботи обговорювались та були схвалені на VII науково-технічній конференція «Інформаційні моделі, системи та технології» (Тернопіль, 2019).

Структура роботи. Дипломна робота складається із вступу, 7 розділів, висновків, списку використаних джерел із 114 найменувань. Робота містить 35 рисунків, 8 таблиць і 4 лістинги. Обсяг основного тексту становить 103 сторінки, бібліографія 12 сторінок. Загальний обсяг дипломної роботи складає 179 сторінок. Ілюстративна частина – 12 слайдів**.**

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі оглядається область, в якій базується це дослідження, закладаючи основи, щоб підкреслити його важливість для ефективних систем моніторингу кібер-інцидентів.

У першому розділі виконується ознайомлення з сучасним рівнем кібербезпеки і кіберзагроз в тому вигляді, в якому вони існують у 2019 році, з метою дати читачеві глибокий контекст в області дослідження.

В загальних рисах описується поточний стан кібербезпеки в світі у 2019 році, який ілюструють ряд атак і атакуючих, що загрожують сучасним системам. Швидке впровадження можливостей зв'язку у системи в результаті феномену «Інтернету речей» досліджується з посиланням на еволюцію загроз, які ці можливості зв'язку використовують.

Також розглядається роль ефективного виявлення вторгнень у захисті систем і пристроїв, наголошуючи на необхідності відмовитися від використання пасивних механізмів виявлення загроз, які все ще широко використовуються в системах. Роль технології Honeypot в забезпеченні активного захисту мережі обговорюється, зокрема, з докладним аналізом важливих характеристик конструкції з метою їх ефективного використання, а також проблем, з якими вони стикаються при широкому поширенні. Нарешті, підкреслюються сильні сторони платформ моніторингу кібер-інцидентів з точки зору підвищення зручності використання і комунікаційних можливостей.

Далі розглядається сучасний стан платформ розгортання, які широко використовуються в виробничих системах, з урахуванням як інфраструктури як послуги (IaaS), так і платформи як послуги (PaaS). Тут до уваги беруться як

можливості, так і проблеми, пов'язані з забезпеченням безпеки в архітектурних системах, які розвиваються.

Далі описано ряд тісно пов'язаних між собою проектів, з якими зіткнулися в ході цього дослідження, виділені їх цікаві атрибути і внесок в область кібербезпеки. Ці проекти по-різному фокусуються на розробці адаптивних приманок, використанні контейнеризації для полегшення їх розгортання та перевагах, які можна отримати від візуалізації даних про загрози.

На основі отриманих знань розглядаються виявлені проблеми при розробленні пропонованої роботи для цього дослідження, а також викладаються основи цілей дослідження.

У другому розділі обговорювались початкові проектні рішення, які були прийняті для задоволення функціональних вимог дослідницького середовища. До них відносяться початкові рішення, що стосуються платформ розгортання, конфігурація мережі Honeynet і проектування системи моніторингу.

Вибір інфраструктури хостингу і платформ для пропонованої системи був важливим фактором при проектуванні, оскільки він справляв значний вплив на успішну розробку монітора кіберінцидентів, а також на пропозицію по розробці адаптивних приманок в цілому. Як платформу для розгортання було обрано Amazon Elastic Compute Cloud, оскільки вона позиціонує як дуже гнучкий засіб швидкого налаштування об’єктів сервера.

Дійшовши висновку, що контейнери є найкращою платформою для розгортання приманок в запропонованій системі, було вирішено, що для реалізації дослідницького середовища буде використовуватися технологія контейнерів Docker. Використання контейнерів Docker, зокрема для реалізації дослідницького середовища, має декілька переваг, зокрема:

1) Кожен контейнер має незалежний мережевий стек, що спрощує реалізацію мережі honeynet в порівнянні з віртуальними мережами.

2) Незалежність і гнучкість ізольованого контейнерного зберігання.

3) Репозиторії Docker, використання яких означає, що строго перевірений образ базової ОС може бути використаний як основа для контейнерів приманок, а потім доповнений налаштованими параметрами конфігурації.

4) Наявність досліджень, що стосуються безпеки технології Docker.

5) Наявність вичерпної документації для екосистеми Docker, а також активна спільнота підтримки.

Приманка Cowrie була визначена як ідеальний варіант для націлювання ботнетів IoT в пропонованому розгортанні, особливо з урахуванням того, що вона є приманкою SSH/telnet, тобто протоколів, які, як було встановлено, найбільш активно використовуються в останніх IoT ботнетах. Той факт, що Cowrie є приманкою середнього рівня взаємодії, означав, що ризики компрометації реальної системи знижуються, а також забезпечується відносно високий рівень інтерактивності з зловмисником

Для передачі журналів між примірниками із забезпеченням їх конфіденційності і цілісності, а також аутентифікації джерела/призначення, було обрано інструмент Filebeat.

Ключовим компонентом пропонованого монітора кіберінцидентів, безсумнівно, є візуалізація, яка покликана підвищити зручність використання та інформаційну цінність шляхом короткого опису даних про атаки, зібрані приманками.

Добре зарекомендованим засобом аналізу, агрегування і візуалізації журналів є стек ELK. Рішення про його використання було прийняте на підставі успішного використання стеку ELK в розробці TPot і того факту, що він схвалений як підхід до візуалізації для приманки Cowrie.

Останнім компонентом системи моніторингу став механізм оповіщення про вторгнення. Найкращим рішенням для запропонованої системи є PSAD – інструмент виявлення вторгнень з відкритим вихідним кодом, який використовується для виявлення сканування портів та іншого шкідливого трафіку в системах Linux.

Для більш повного задоволення вимог пропонованої системи розглядався ряд виявлених пробем, які вимагають додаткового аналізу. Зокрема, це проблеми щодо зняття відбитків системи в середовищі приманок, питання збереження вмісту енергонезалежного контейнера, міркування щодо безпеки використання Docker, проблема заохочення атак IoT ботнетів та їх виявлення поміж інших атакуючих, а також деякі етичні проблеми.

Також розділ містить зведення, в якому, зокрема, визнається непередбачуваний характер досліджень у міру їх розвитку.

У третьому розділі описується реалізація різних компонентів дослідницької середовища, зокрема веб-сервісу AWS EC2, приманок Cowrie, контейнерної екосистеми Docker, а також інструментів для обробки та візуалізації журналів. В інтересах стислості, низькорівневі деталі встановлення інструментів та ін. не пояснюється в деталях. Замість цього, основна увага приділяється впровадженню компонентів системи та докладному описі прийнятих рішень при зіткненні з проблемами.

Спершу описується процес розгортання і налаштування правил безпеки двох екземплярів EC2 – примірник сервера-приманки та примірник сервера управління. Згодом, перш ніж інкапсулювати приманку Cowrie в контейнерне середовище, розглядається її базова конфігурація і налаштування. Щоб отримати дані логування, приманка була налаштована і відкрита для публічного Інтернету. Cowrie був налаштований з ім'ям, яке відповідає конкретній моделі IP-камери TPLink, а саме TPLink-TL-SC3171, так як після проведення короткого веб-пошуку ця модель була відразу ж ідентифікована як з вразливістю віддаленого виконання коду (RCE).

Щоб зрозуміти принцип побудови контейнерних середовищ і того, як з ними взаємодіяти, перш ніж перейти до реалізації контейнерної мережі Honeynet, було розглянуто базовий вихідний код Docker-Cowrie, наданий розробниками Cowrie. Згодом, за допомогою Docker було розгорнуто мережу приманок Honeynet.

В ході налаштування контейнера Honeywall було виявлено, що Cowrie немає можливостей вихідної мережі, тому він не може встановлювати вихідні з'єднання SSH або telnet. Цей факт не був відомий на початку дослідження, тому система вимагала переоцінена. Було прийняте рішення запровадити нову приманку з високим рівнем взаємодії для полегшення поширення атак за межами Honeywall –

контейнер маршрутизатора (router). Налаштування, а також проблеми, які виникали в процесі, описуються в деталях.

Після встановлення всіх необхідних компонентів було виконано перевірку конфігурації мережі Honeynet. Для цього на контейнерах налаштовувалась маршрутизація, яка згодом перевірялась за допомогою консольних команд.

Для візуалізації даних атаки на примірник сервера управління було встановлено і налаштовано стек обробки журналів ELK. Щоб полегшити використання його для аналізу журналів з віддаленого комп'ютера також використовувалися деякі додаткові інструменти: зокрема, Nginx і Filebeat. Також була налаштована системи сповіщень про загрозу (PSAD).

На той час, коли всі компоненти системи були сконфігуровані і реалізовані, були досягнуті такі цілі:

1) Сеанси атаки можна змоделювати, підключившись до примірника приманки EC2 по SSH або telnet і представивши його в запрошенні на вхід в контейнер маршрутизатора. Після аутентифікації в контейнері маршрутизатора стало можливим аналогічним чином підключатися до будь-якого контейнера в мережі Honeynet і взаємодіяти з приманками Cowrie.

2) Вся згенерована діяльність із взаємодій з контейнерами Cowrie була успішно відправлена, оброблена і візуалізована за допомогою панелі візуалізації, яка доступна з веб-браузера.

3) При необхідності, все середовище Docker може бути повністю вилучене і повторно розгорнуте з ідентичною конфігурацією.

Таким чином, мета розробки монітора кібер-інцидентів, який керується приманкою, була в значній мірі досягнута.

У спеціальній частині основна увага приділяється оцінці реалізованої системи моніторингу кіберінцидентів, а також опису планування та проведення експериментів як частини пропозиції щодо проектування адаптивної приманки.

Проведення експериментів було сфокусоване на визначені покращеної структуру для ефективних адаптивних приманок. Міра ефективності в цих експериментах залежала від того, скільки атак отримала кожна з приманок.

Для проведення експериментів була розроблена таблиця ітерацій, в які вказувались змінні і постійні налаштування приманок для кожного тижня. Детально описано характер численних невдач і як з ними справлятися. Пояснення до раннього завершення експериментів також надається. На основі отриманих результатів робляться деякі важливі висновки.

В розділі «Обґрунтування економічної ефективності» здійснено розрахунок економічної ефективності дипломного проекту та термін окупності капітальних вкладень.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання створення метеорологічних умов виробничого середовища і захист від шумів, вібрацій, випромінювань у виробничих приміщеннях з ЕОМ.

В розділі «Екологія» розглянуто питання щодо екологізації та статистичного аналізу тенденцій і закономірностей динаміки в екології.

У загальних висновках щодо дипломного проекту описано результати розробки системи моніторингу кіберінцидентів, зроблено висновок щодо контейнеризації додатків безпеки та викладено деякі міркування стосовно майбутнього IoT пристроїв.

ВИСНОВКИ

Основним внеском в цій дипломній роботі стало розроблення нового контейнерного монітора кіберінцидентів, який керується мережею приманок і дозволяє системним адміністраторам представляти дані загроз осмисленим чином, забезпечуючи цілісне уявлення про свої системи.

Існують переконливі докази того, що монітор інцидентів, розроблений в цьому дослідженні, забезпечує більшу придатність даних приманок, ніж той, який був би отриманий тільки при їх використанні:

- Візуалізація даних приманок означає, що немає потреби переглядати великі обсяги журналів, щоб зрозуміти найбільш актуальну інформацію про загрози;
- Агрегування даних з декількох приманок за допомогою централізованої системи реєстрації даних, що дозволяє легко ідентифікувати тенденції загроз;
- Можливість отримувати миттєві оповіщення про загрози по електронною поштою;
- Встановлення та налаштування приманок та мережі, необхідної для їх підключення, повністю автоматизоване.

Таким чином, ця розробка ефективно усуває багато з основних перешкод на шляху до використання активного мережевого захисту в інфраструктурі, що, безумовно, є цінним внеском в область кібербезпеки.

Цінність рішення мережі приманок, яка була реалізована в цій роботі, значно підвищило використання контейнерів. Вони служать перевіркою концепції щодо зручності використання активних механізмів захисту мережі для мережевих адміністраторів, надаючи можливість автоматичного встановлення і налаштування кількох середовищ «на льоту».

Як спостерігалось з цього дослідження, контейнеризація додатків безпеки викликає досить багато супутніх проблем, основним чином через відсутність інструкцій та ресурсів, якими можна було б керуватись при розробці таких систем. Тому ця область сповнена напрямків для досліджень і оцінки різних підходів.

Робота з приманками може бути вкрай непередбачуваною, що ускладнює проведення переконливих досліджень в умовах браку часу. Однак, очевидно, що здатність забезпечувати активний захист мережі за допомогою обману і моніторингу дій зловмисників робить їх привабливим варіантом для боротьби з динамічними загрозами, які все виникають все частіше. Об’єкти критичної інфраструктури гостро потребують адаптивних можливостей приманок до виявлення загроз для захисту своїх систем і тих, хто від них залежить.

Навіть з обмежених експериментів, які проводилися в цьому дослідженні, ясно, що ботнети IoT є надзвичайно активними: кожна «річ» з підключенням до Інтернету є засобом використання комунікацій та взаємодії. Люди все більше залежать від взаємопов'язаних служб і додатків і, як наслідок, стають вразливими для кіберзагроз, які перебувають поза досяжністю їх власних пристроїв.

Об’єкти критичної інфраструктури будуть піддаватися серйозним кібератакам і надалі, оскільки кібервійни між різними державами у світі тривають. Однак, перш ніж ці проблеми зможуть бути вирішені, є необхідними величезні інновації в галузі безпеки IoT: тільки коли система спроектована з урахуванням вимог безпеки, її можна вважати відносно безпечною. Замість цього додатки продовжують отримувати інтегровану в них можливість з'єднання з дуже невеликою увагою до безпеки. Цілком ймовірно, що до тих пір, поки у виробників не з'явиться дійсно ринковий стимул для впровадження гідних механізмів безпеки у своїй продукції, ситуація навколо пристроїв «Інтернету речей» навряд чи зміниться.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Виявлення загроз для IoT-пристроїв засобами Honeypots [Текст] / Збірник тез VII науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» – Тернопіль (11-12 грудня 2019 року), ТНТУ, 2019. – с. 23.

АНОТАЦІЯ

В даній роботі були досліджені методи розробки адаптивних контейнерних приманок для моніторингу інцидентів інформаційної безпеки. В результаті дослідження було розроблено систему для консолідації і моніторингу інформації, отриманої з мережі приманок, а також розглянуто адаптацію приманок для залучення атак.

Ключові слова: приманка, мережа приманок, моніторинг, консолідація, контейнер, інформаційна безпека.

ANNOTATION

The methods of developing of adaptive containerized honeypots for Cyber-Incident monitoring were investigated in this thesis. As a result, a system for consolidating and monitoring information obtained from a honeynet was developed and the adaptation of honeypots to attract attacks was also considered.

Keywords: honeypot, honeynet, monitoring, consolidation, container, information security.