Міністерство освіти та науки України
Національна академія наук України
Люблінський відділ Польської Академії Наук
Представництво «Польська академія наук» у Києві
Харківський національний університет радіоелектроніки
AGH науково-технологічний університет ім. Ст. Сташіца в Кракові
Прикарпатський національний університет ім. В. Стефаника
Національний університет кораблебудування ім. адмірала Макарова
Запорізький національний університет
Академія Наук Прикладної Радіоелектроніки
Одеський національний політехнічний університет
Українська нафтогазова академія
Українська Федерація Інформатики
Білоруський державний університет інформатики та радіоелектроніки
Білоруський національний технічний університет

«Інформаційні системи та технології»
ICT-2020

М А Т Е Р І А Л И
**9-ї Міжнародної науково-технічної конференції,
присвяченої 90-річчю
Харківського національного університету радіоелектроніки**

**17-20 листопада 2020 р.
Харків, Україна**

«INFORMATION SYSTEMS AND TECHNOLOGIES»
IST-2020

Proceedings
of the 9-th International Scientific and Technical Conference
dedicated to the 90th anniversary
of Kharkiv National University of Radio Electronics

November 17-20, 2020
Kharkiv, Ukraine

Харків 2020

УДК: 004.9

І-74

Наукові редактори: *А. Д. Тевяшев – доктор технічних наук, професор (Харківський національний університет радіоелектроніки);*
Л. Б. Петришин – доктор технічних наук, професор (AGH University of Science and Technology, Прикарпатський національний університет ім.В.Стефаника);
В. Г. Кобзєв – кандидат технічних наук, старший науковий співробітник (Харківський національний університет радіоелектроніки)

Рецензенти:
Секція 1. *В. О. Філатов – доктор технічних наук, професор (Харківський національний університет радіоелектроніки);*
Секція 2. *В. В. Безкоровайний – доктор технічних наук, професор (Харківський національний університет радіоелектроніки);*
Секція 3. *Ю. О. Гунченко – доктор технічних наук, професор (Одеський національний університет ім. І. І. Мечникова);*
Секція 4. *В. П. Машталір – доктор технічних наук, професор (Харківський національний університет радіоелектроніки);*
Секція 5. *О. О. Шумейко – доктор технічних наук, професор (Дніпровський державний технічний університет);*
Секція 6. *Н. В. Шаронова – доктор технічних наук, професор (Національний технічний університет «ХПІ»);*
Секція 7. *О. В. Бісікало – доктор технічних наук, професор (Вінницький національний технічний університет);*
Секція 8. *В. А. Лужецький – доктор технічних наук, професор (Вінницький національний технічний університет);*
Секція 9. *Є. В. Бодянський – доктор технічних наук, професор (Харківський національний університет радіоелектроніки)*

І-74 **Інформаційні системи** та технології: матеріали статей 9-ї Міжнародної науково-технічної конференції, Харків, 17-20 листопада 2020 року / наук. ред. А. Д. Тевяшев, Л. Б. Петришин, В. Г. Кобзєв. – ХНУРЕ. – Х.: Друкарня Мадрид, 2020. – 313 с.

ISBN 987-617-7988-25-9

Збірник містить матеріали статей Міжнародної науково-технічної конференції з проблем сучасних інформаційних систем та технологій.
Матеріали представляють інтерес для фахівців, науковців і аспірантів, діяльність яких пов'язана з розробкою та впровадженням сучасних інформаційних систем і технологій.

УДК: 004.9

Матеріали статей рецензовано та опубліковано в авторській редакції

ISBN 987-617-7988-25-9

З М І С Т

Секція 4. Розпізнавання образів, цифрова обробка зображень і сигналів

Секція 8. Захист інформації. Інформаційна безпека

Секція 9. Інтелектуальний аналіз даних, Data Mining та Big Data-технології

Section 8. Intellectual data analysis, Data Mining and Big Data technologies 283

Інформаційна Модель Системи Технічного Захисту Інформації на Основі Технології Honeypot

Максим Левченко
кафедра комп'ютерних технологій та інформаційної безпеки
Національний університет кораблебудування імені адмірала Макарова
Миколаїв, Україна
maxivelp@gmail.com

Марина Турти
кафедра комп'ютерних технологій та інформаційної безпеки
Національний університет кораблебудування імені адмірала Макарова
Миколаїв, Україна
turtym@meta.ua

Information Model of Technical Information Protection System Based on Honeypot Technology

Maksym Levchenko
Department of Computer Technologies and Information Security
Admiral Makarov National University of Shipbuilding
Mykolaiv, Ukraine
maxivelp@gmail.com

Marina Turty
Department of Computer Technologies and Information Security
Admiral Makarov National University of Shipbuilding
Mykolaiv, Ukraine
turtym@meta.ua

***Анотація* — Проведено огляд сучасних технологій і засобів Honeypot. Визначені казуальні зв'язки функцій, виконуваних Honeypot і інформаційних потоків в системі обробки та захисту інформації. Створена узагальнена інформаційна модель системи технічного захисту інформації на основі технології Honeypot, яка враховує особливості віртуальних приманок.**

***Abstract* — The modern technologies and tools Honeypot have been reviewed. The casual connections of the functions performed by Honeypot and information flows in the information processing and protection system have been determined. A generalized information model of the technical information protection system based on Honeypot technology has been created, which takes into account the features of virtual lures.**

Ключові слова — Honeypot, інформаційна безпека, віртуальна приманка, механізм виявлення атак, узагальнена інформаційна модель.

Keywords — Honeypot, information security, virtual lure, attack detection mechanism, generalized information mode.

I. Вступ

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Одна з найважливіших задач, яку доводиться вирішувати фахівцям з кібербезпеки - це збір відомостей, що дозволяють виявити атаки, зрозуміти як вони спрацьовують і чому. Спершу сутність кіберзагроз намагалися з'ясувати, аналізуючи програми, використані для несанкціонованого доступу, згодом після того як трапився інцидент, єдині дані, на які могли розраховувати експерти – це інформація, що збереглася в зламаній системі. На жаль, вона надзвичайно небагата і недостатньо повно може сказати про небезпеку в цілому [1-3]. Виявлення атак на базі віртуальних приманок, зокрема Honeypot, дозволяє значимо розширити інформацію про напад і про атакуючого [4-8].

Honeypot може вирішувати в архітектурі системи безпеки різноманітні задачі, спектр яких залежить від побудови засобів Honeypot, їх налаштувань та способів

використання. Призначення Honeypot полягає в тому, щоб стати дослідженим або бути атакованим зловмисником.

II. Аналіз літературних джерел та постановка проблеми

Протягом останніх двадцяти років основні дослідження Honeypot проводяться Honeynet Project. Honeynet Project - це міжнародна неприбуткова організація з досліджень безпеки, яка займається розслідуванням сучасних атак та розробкою інструментів безпеки з відкритим кодом для покращення Інтернет-безпеки [9]. Організація:

- має мережу волонтерів, які виявляють і вивчають нові атаки, оприлюднюють отримані результати досліджень та створюють на їх основі новітні інструменти безпеки;
- проводить щорічні конференції;
- щорічно формує перелік актуальних проектів, кожен з яких має власного куратора і низку вимог до бажаючих увійти в групу волонтерів-розробників проекту.

Так поточними проектами 2020 р. є наступні розробки.

- Thug – засіб взаємодії Python із низькою взаємодією, спрямований на імітацію поведінки web-браузера з метою виявлення та емуляції шкідливого вмісту;
- T-POT – засіб, який базується на демонах Honeypot, IDS та інструментах для подання атак і дозволяє створити систему, у якій весь діапазон мережі TCP, а також деякі важливі служби UDP виступають у ролі медоносної точки, тобто весь вхідний трафік атак спрямовується на спеціалізовані демони з метою обробки і реагування;
- Mitmproxy – засіб налагодження і тестування конфіденційності, що може бути використаний для перехоплення, перевірки, модифікації та відтворення web -трафіку, такого як HTTP/1, HTTP/2, WebSockets або будь-яких інших протоколів, захищених SSL/TLS. Він дозволяє впорядковувати та декодувати різні типи повідомлень, починаючи від HTML і закінчуючи Protobuf, перехоплювати конкретні повідомлення на льоту, модифікувати їх до того, як вони досягнуть місця призначення, і відтворювати їх на клієнт або сервер пізніше;
- Snare and Tanner – це двокомпонентний засіб. Snare - це датчик веб-додатків Honeypot, а Tanner реалізує послугу віддаленого аналізу та класифікації даних для оцінки запитів HTTP та складання відповіді, яку потім обслуговує Snare. Tanner використовує різні методи емуляції типу вразливості при наданні відповідей для Snare;
- Intel Owl – це рішення OSINT для отримання даних розвідки про загрози щодо конкретного файлу, IP-адреси або домену з одного API у масштабі. Він інтегрує ряд аналізаторів, доступних в Інтернеті, і призначений для випадків, коли потрібна одна точка для запиту інформації про конкретний файл або для спостереження;
- Glutton - загальний Honeypot із взаємодією низького рівня;
- Dockpot – Honeypot із взаємодією високого рівня. Це високоякісний SSH-пакет, заснований на Docker, який може діяти як проксі-сервер SSH між зловмисником та Honeypot (із Docker-контейнером) та реєструвати діяльність зловмисника.
- Conpot – Honeypot із взаємодією низького рівня на боці сервера ICS. Conpot орієнтований на використання у промислових системах і забезпечує легкість розгортання, модифікації та розширення системи. Conpot дозволяє користувачу побудувати власну систему на стеках протоколів, здатну наслідувати складну інфраструктуру, щоб переконати зловмисника в тому, що він щойно знайшов величезний промисловий комплекс. Для поліпшення оманливих можливостей використовується сервер спеціального людинно - машинного інтерфейсу. Зокрема, час відгуку служб може бути штучно відкладено, щоб зімітувати поведінку системи під постійним навантаженням;
- Droidbox – це платформа динамічного аналізу (пісочниця) для додатків Android. В результаті аналізу визначаються: хеші для аналізованого пакету; вхідні/вихідні дані мережі; операції зчитування та запису файлів; запущені служби та завантажені класи через DexClassLoader; витік інформації через мережу, файли та SMS; дозволи; криптографічні операції, що виконуються за допомогою Android API; перелік широкосповіщувальних приймачів; надіслані SMS та телефонні дзвінки. Крім того, генеруються два графіки, що візуалізують поведінку пакета: перший графік показує часовий порядок операцій, а другий - деревоподібну карту, яку можна використовувати для перевірки схожості між аналізованими пакетами;
- Dionaea – це Honeypot із взаємодією низького рівня, що призначений для виявлення атак на корисне навантаження, помилок та шкідливого програмного забезпечення. Dionaea вбудовує Python як мову скриптів, використовує бібліотеки для виявлення кодів оболонки, підтримує ipv6 та tls.

Проведений аналіз літературних джерел [1-9] дозволяє зробити висновок, що Honeypot може виконувати в системі захисту інформації унікальні функції і є корисним інструментом для виявлення, розслідування та попередження інцидентів інформаційної безпеки. Оцінювання ефективності такого інструменту повинне базуватися на детальному аналізі інформацій них потоків в системі «Зловмисник – Система захисту інформації (СЗІ) – Система обробки інформації».

III. Мета і задачі дослідження

Метою даної роботи є побудова інформаційної моделі системи технічного захисту інформації на основі технології Honeypot.

Для досягнення поставленої мети необхідно розв'язати ряд задач: провести аналіз існуючих систем Honeypot; визначити казуальний зв'язок функцій, виконуваних Honeypot і інформаційних потоків в системі обробки та захисту інформації; розробити інформаційну модель системи захисту інформації на основі технології Honeypot.

IV. Аналіз систем Honeypot

Залежно від завдань, поставлених перед засобами Honeypot, вони поділяються на виробничі і дослідницькі Honeypot.

Виробничі Honeypot допомагають знизити ризик в організації або середовищі шляхом попередження, виявлення і протоколювання деструктивних впливів.

Дослідницькі Honeypot в загальному випадку не зменшують поточний ризик для організації, але вони надають платформу для вивчення загроз і дозволяють отримати інформацію, яка надалі може бути застосована в реальних системах для поліпшення попередження, виявлення, можливостей протоколювання і необхідної реакції. Вони дозволяють не тільки знаходити використані зловмисником засоби, а й бачити (аж до натискання клавіш), як саме зловмисник досліджує систему і починає атаку. Дослідницькі Honeypot можуть бути застосовані:

- при збиранні інформації про автоматизовані загрози, таких як мережеві хробаки . Швидкий збір інформації позитивно впливає на швидкість реакції та подальшу нейтралізацію даних загроз;
- як предиктивний механізм. Дані, що збираються Honeypot, можуть бути використані для статистичного моделювання, передбачення нових варіантів атак, і відповідного вдосконалення СЗІ;
- для виявлення раніше невідомих засобів і технік для здійснення атак і формування образів нових атак;
- для поліпшення розуміння мотивацій і організації зловмисників. Завдяки збору інформації під час здійснення атаки, наприклад, варіантів переговорів зловмисників між собою, можна відповісти на питання, хто є загроза і навіщо проводиться атака;
- для збирання інформації про зловмисників високої кваліфікації.

За рівнем взаємодії із зловмисником розрізняють три основних види Honeypot: слабкої взаємодії; середньої взаємодії і сильної взаємодії.

Засоби Honeypot слабкої взаємодії зазвичай досить просто встановити, налаштувати, використовувати і підтримувати, тому що вони мають просту структуру і базові функції. Як правило, такі Honeypot імітують тільки частину сервісів, і зловмисник обмежений у взаємодії з цими сервісами. Засоби Honeypot цього типу надають тільки транзакційну інформацію про зловмисника, тобто інформацію про обставини атаки, але не про саму атаку: час і дата атаки; IP-адреса і порт джерела (зловмисника); IP-адреса і порт призначення (засоби Honeypot). Honeypot слабкої взаємодії показують поганий або навіть негативний результат при взаємодії з невідомими або непередбачуваними видами атак.

Засоби Honeypot сильної взаємодії надають зловмисникові доступ до реальної операційної системи, де нічого не імітується або не обмежується. В даному випадку є можливість досліджувати нові засоби, виявляти нові уразливості в операційних системах або додатках, а також дізнаватися, яким чином зловмисники зв'язуються між собою. Такі засоби надають найбільшу кількість інформації про зловмисників, але вимагають достатній час для побудови і підтримки, і є дуже чутливими до похибок налаштувань. У більшості випадків Honeypot сильної взаємодії розташовуються в контрольованому середовищі, наприклад, в мережі - після брандмауера. Міжмережевий екран надає зловмисникові можливість атакувати засіб Honeypot, але забороняє здійснювати зовнішні атаки. Системи виявлення вторгнень також, можуть бути також включені у Honeypot сильної взаємодії.

Засіб Honeypot середньої взаємодії надає зловмисникові більше можливостей, ніж Honeypot слабкої взаємодії, але має меншу функціональність у порівнянні з Honeypot сильної взаємодії. Дані засоби можуть очікувати різну активність зловмисника і давати кілька можливих відповідей на його дії. Наприклад, якщо імітується IIS Web Server, то Honeypot може бути налаштований з різною функціональністю і поведінкою, щоб виявляти певного мережного хробака. Даний рівень взаємодії вже вище, ніж у Honeypot слабкої взаємодії, де присутній тільки HTTP-банер. При цьому є можливість зібрати інформацію щодо поведінки хробака для подальшого аналізу. Йому не надається повноцінна операційна система, що знижує ризик. Існує тільки додаток що імітується.

Починаючи від Honeypot слабкої взаємодії, функціональні можливості Honeypot розширюються. Відповідно змінюються: процес установки і налаштування, процес використання і підтримки, обсяг і процес збирання даних, рівень протоколювання, рівень імітації і рівень ризику.

Структура і спектр виконуваних Honeypot функцій визначаються призначенням Honeypot:

- якщо необхідно вивчити мотивації поведінки зловмисників, методи їх атак і засобів - тоді потрібно побудувати складний Honeypot, який надає зловмисникові повноцінну операційну систему, з якою він буде взаємодіяти, і забезпечити високий рівень протоколювання.
- якщо необхідно виявити несанкціоновану активність, таку як сканування системи, то для цих цілей можна побудувати простий Honeypot, який

буде імітувати мінімальні можливості і операції сервісів, записуючи лише команди взаємодії зі зловмисником.

- якщо ставиться завдання виявити мережного хробака для аналізу, тоді буде потрібно побудувати гнучкий Honeypot, який буде взаємодіяти з хробаком, збираючи елементи його активності.

V. Розробка інформаційної моделі системи захисту інформації на основі технології Honeypot

При розробці інформаційної моделі були враховані наступні функціональні вимоги до засобів Honeypot:

- можливість вибору варіанту імітованого сервісу (наприклад, вибір різного FTP-сервера);
- максимальне наближення до імітованого сервісу: особливості роботи; реакція на стандартні / нестандартні команди або запити; підтримка реалізованих додаткових можливостей обраного сервісу;
- існування можливості (або умов) емуляції злому сервісу;
- відповідність поточному (сучасному) набору вразливостей. Під набором вразливостей розуміється сукупність відомих вразливостей для даного сервісу, а також набір варіантів аномального поведінки при взаємодії з імітованим сервісом. Таким чином, Honeypot повинен містити набори вразливостей для кожного імітованого сервісу та аналітичний модуль прийняття рішень для встановлення факту злому або наявності аномального поведінки при взаємодії з імітованого сервісом;
- існування бази даних (БД) для зберігання наборів вразливостей, з можливістю зміни і доповнення.
- захист БД наборів вразливостей від додаткових загроз (можливість реалізації атаки на інші, не імітовані сервіси, в результаті якої властивості цілісності і конфіденційності БД наборів вразливостей будуть порушені). Одним з головних вимог по даному пункту є вимога розміщення БД вразливостей на іншому хості;
- повне протоколювання взаємодії потенційного порушника з Honeypot. Протокол повинен містити як інформацію, яка була отримана від порушника, так і відповідь імітованого сервісу, який був відісланий порушнику.

Структурна схема розробленої узагальненої інформаційної моделі наведена на рис.1.

VI. Висновки

Таким чином, в даній роботі на основі проведеного аналізу сучасних систем Honeypot визначені основні функції віртуальних приманок, казуальні зв'язки цих функцій з інформаційними потоками, і розроблена інформаційна модель системи захисту інформації на основі технології Honeypot.

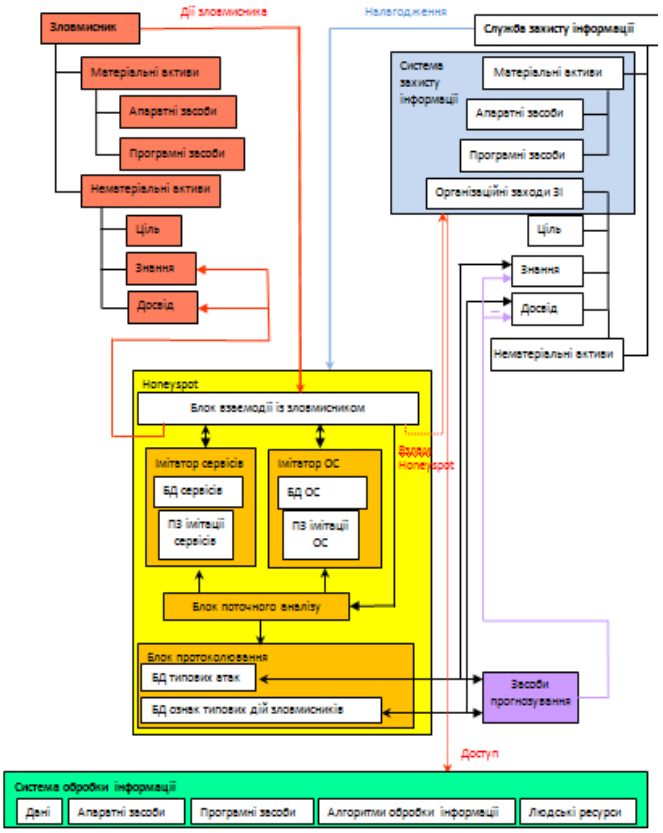

Рис.1 Структурна схема інформаційної моделі Honeyspot

Література References

[1] V.L. Buryachok, “Informatsiyna ta kiberbezpeka: sotsiotekhnichnyy aspekt”. K., DUT, 2015, 288 p.

[2] V.L. Buryachok, V.A. Kozachok, L.V. Buryachok, P.M. Skladannyy ”Pentestinh yak instrument kompleksnoyi otsinky efektyvnosti zakhystu informatsiyi v rozpodilenykh korporatyvnykh merezhakh”. *Suchasnyy zakhyst informatsiyi*, №3, pp. 4-12, 2015 . [Online]. Available: http://nbuv.gov.ua/UJRN/szi_2015_3_3.

[3] S.O. Hnatyuk, Yu.Ye. Khokhlachova, A.O. Okhrimenko, A.K Hreben′kova. ”Teoretychni osnovy pobudovy ta funktsionuvannya system upravlinnya intsydentamy informatsiynoyi bezpeky”. *Zakhyst informatsiyi*, vol.14, №54, pp.120-126, 2012.

[4] “Honeypots: Monitoring and Forensics” (2002). . [Online]. Available: http://honeypots.sourceforge.net/monitoring_vmware_honeypots.html.

[5] L. Spitzner, “Dynamic Honeypots” (2003). [Online]. Available: https://www.researchgate.net/publication/271070241_Design_and_Implementation_of_a_Medium_Interaction_Honeypot..

[6] L. Spitzner, “Honeypots: TrackingHackers. AddisonWesley” (2002). . [Online]. Available: http://www.it-docs.net/ddata/792.pdf.

[7] R.A. Grimes, “Honeypots for Windows. Apress” (2004). [Online]. Available:: http://docplayer.net/5623194-Honeypots-for-windows-roger-a-grimes.html.

[8] “The Honeynet Project. Know Your Enemy: Learning about Security Threats” (2003). . [Online]. Available: http://old.honeynet.org/papers/honeynet.

[9] “Google Summer of Code 2020 Project Ideas” (2020). [Online]. Available: https://www.honeynet.org/gsoc/gsoc-2020/google-summer-of-code-2020-project-ideas/

Наукове видання

«Інформаційні системи та технології» ІСТ-2020

М А Т Е Р І А Л И
9-ї Міжнародної науково-технічної конференції

17-20 листопада 2020

Харків, Україна

«INFORMATION SYSTEMS AND TECHNOLOGIES» IST-2020

Proceedings
of the 9-th International Scientific and Technical Conference

November 17-20, 2020

Kharkiv, Ukraine

Наукові редактори: А. Д. Тевяшев, Л. Б. Петришин, В. Г. Кобзєв
Коректор – Н. Р. Сухина
Комп'ютерна верстка – Ю. В. Міщеряков, Т. Є. Сергієнко

Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14,
ХНУРЕ

Підписано до друку 20.11.2020.
Папір 80 г/м^2.
Умов.-друк. арк. – 36,38. Обл.-вид. арк. – 26,16.
Наклад 150. Зам. № 007.

Видавець і виготовлювач ТОВ «ДРУКАРНЯ МАДРИД»
через ФОП Дудінова О. Б.
61024, м. Харків, вул. Гуданова, 18
Тел.: (057) 756-53-25
www.madrid.in.ua info@madrid.in.ua