УДК 004.056.5 DOI: 10.26565/2519-2310-2020-1-03

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ТЕХНОЛОГІЇ HONEYPOT

Тетяна Кохановська, Олексій Нарежний, Олександр Дьяченко

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
tanya.koh99@gmail.com, o.nariezhnii@karazin.ua, diachenko4@gmail.com

Рецензент: Олександр Оксіюк, д.т.н., проф., Київський національний університет імені Т. Шевченка, вул. М. Ломоносова 81, Київ, 03189, Україна.
o.oksiuk@gmail.com

Поступила: Березень 2020.

Анотація: *Визначено роль та головні завдання різних мережевих пасток (Honeypot) при побудові інтегрованих систем безпеки. Розглянуто основні класифікаційні ознаки та особливості первинних налаштувань декількох комерційних засобів. Зроблено висновок, що основні переваги технології Honeypot, серед іншого, полягають в їх гнучкості та масштабованості. Підкреслено, що на даний час поки ще немає досконалих методик ідентифікації і швидкої компрометації мережевих паст. Звернено увагу на те що, тактика мережевої розвідки і методи здійснення мережевих атак постійно прогресують. Враховуючи цей факт постійний аудит даних Honeypot і оперативна реакція на визначені мережеві інциденти та колізії є одним із головних напрямків роботи для фахівців з питань забезпечення вимог корпоративної політики інформаційної безпеки. Відзначено, що архітектура різних пасток, в цілому, достатньо добре відома і тому є потенційно вразливою. Тому, наділяючи пастки більш гнучким (варіативним) сценарним контекстом та скорочуючи час мережевої експозиції можливо підтримувати їх захистний потенціал в досить паритетному стані. Ці обидва напряму потребують більш щільної уваги (докладний аналіз даних log-файлів та корегування алгоритмів роботи поведінкового аватару для створеної пастки) зі сторони персоналу, та вимагають постійної підтримки його професійних компетенцій. За результатами огляду можливостей існуючих Honeypot та узагальнення типових ознак мережевої активності найбільш характерних вузлів (в даному випадку файлового серверу), розглянуто особливості синтезу відповідних поведінкових профілів (аватарів) для корегування роботи програмних пасток. Стверджується, що систематизація правил роботи аватару Honeypot (як сукупності користувальницьких поведінкових алгоритмів) та своєчасна корекція наявних баз поведінкових профілів є завдання, яке важко формалізується. Це обумовлено потенційним різноманіттям варіантів мережевої активності, що притаманна для кожної конкретної мережі та налаштувань наявних мережевих вузлів. В цьому сенсі надлишкова уніфікація (звуження можливого поля поведінкових реакцій) поведінкових профілів Honeypot в значної мірі може полегшити зловмиснику проведення моніторингу та наступної ідентифікації створеної пастки. Тому формування базового набору відповідних мережевих аватарів слід розглядати, не більше, як основу для її подальшої модифікації під специфіку завдань, топологію та інші особливості кожної окремої IT-структури (або особливості їх окремих елементів). Підкреслено, що впровадження технології пасток не підміняє собою інших технологій і інструментів безпеки, а лише ефективно розширює наявний арсенал протидії новим загрозам безпеки (перш за все, як інструмент швидкого реагування). Тому шлях інтеграції Honeypot з іншими, вже розгорнутими рішеннями ІБ, є найбільш збалансованим напрямом для подальшого підвищення загального рівня безпеки мережевих ресурсів.*

Ключові слова*: Honeypot; вторгнення; інформаційна безпека; ЛОМ; Firewall; IDS; IPS.*

1 Вступ

На сьогодняшний день більша частина людства активно користується Інтернетом, а кожна сучасна людина, в той чи іншої мірі є користувачем персонального комп'ютера (ПК) або якогось іншого електронного гаджету. Паралельно зі стрімким розвитком усіх основних напрямків інформаційних технологій (ІТ) постійно вдосконалюються і різноманітні технології проведення мережевих атак та ведення кібершпіонажу. Це напрямок діяльності створює постійну загрозу для безпеки інформаційних ресурсів і є основним спонукальним чинником для організації ефективних заходів протидії різнорідним мережевим загрозам. Саме тому, на постійній основі, необхідно забезпечувати комплексний моніторинг всієї поточної мережевої активності, особливо в частині аналізу змісту, характеру та інтенсивності трансграничного трафіку. Це в першу чергу стосується аналізу трафіку в межах спеціально передбачених демілітаризованих зон та відповідних публічних сервісів (при їх наявності), що передбачають інтенсивну взаємодію з користувачами, які знаходяться за рамками організованого периметра безпеки компанії або окремого користувача. Одним з ефективних засобів ведення моніторингу поточної мережевої активності та виявлення ознак підготовки майбутнього кіберзло-

чина, є використання можливостей технології Honeypot (т.з. вузлів або мереж пасток/приманок). Мета даної роботи полягає у аналізі основних можливостей існуючих Honeypot, та розгляді особливостей подальшого розвитку мережевих пасток, що впроваджують тактику адаптивної протидії (*використання поведінкових сценаріїв*).

2. Особливості функціонування та питання класифікації Honeypot

Honeypot (*з англ. - «горщик з медом»*) - програмно-апаратний ресурс, який представляє собою функціональну приманку (або пастку) для потенційних мережевих зловмисників, яка відповідним чином розміщена, налаштована та періодично обслуговується для забезпечення її більш ефективного використання за призначенням [1]. Honeypot (далі HPot) помітно відрізняється від інших поширених технологій забезпечення інформаційної безпеки (ІБ). Так, більшість технологій забезпечення ІБ, що використовуються сьогодні, було спроектовано для вирішення якоїсь однієї задачі [2]. Наприклад, міжмережевий екран (ММЕ) контролює вхідний і вихідний мережевий трафік і використовується, переважно, як засіб блокування будь-якої несанкціонованої мережевої активності (*в т.ч. трафіку*). Системи виявлення вторгнень (*IDS - Intrusion Detection System*) визначають атаки, здійснюючи постійний моніторинг мережі і системної активності користувачів, а мережевий комутатор підтримує адміністрування трафіку згідно створеного для нього ACL (*Access Control List*) і т.і. В цьому сенсі HPot відрізняється від класичних засобів забезпечення ІБ, таких як ММЕ, IDS або систем захисту від витоку даних [2,3] тим, що вони не покликані вирішувати будь-яку конкретну задачу. Навпаки, HPot - гнучкий засіб, який може бути застосовано в різних ситуаціях та в різних масштабах (*точково, використовуючи розподілену структуру або реалізуючи гібридне рішення*). Так наприклад, засоби HPot можуть дозволяти запобігати або виявляти атаки, або тільки імітувати роботу певного ресурсу (*окремого серверу або цілої Scatternet*). Таким чином, HPot поєднують в собі (*в залежності від конкретних завдань, що на них покладені у кожному конкретному випадку*) деяку функціональність практично всіх засобів забезпечення ІБ.

HPot вперше з'явилися з першими комп'ютерними зловмисниками, а роботи по їх створенню та практичному впровадженню проводилися паралельно з дослідженнями *IDS* та *IPS* (*Intrusion Prevention System*, та її різновид *WIPS - Wireless Intrusion Prevention System*). Першою документальною згадкою, за тематикою HPot, була робота Кліффорда Столла *«The Cuckoo's Egg»*, що вийшла у 1990 році. А вже у 2000-х роках HPot стали досить поширеними елементами інтегрованих систем безпеки, що забезпечували ефективну протидію спробам несанкціонованого проникнення до «внутрішнього» периметру безпеки комп'ютерних мереж компаній і установ [1].

В спрощеному трактуванні основне завдання HPot – навмисно виявитися та піддатися атаці зі сторони сторонньої особи або зовнішнього програмного засобу (ПЗ), що згодом дозволить вивчити стратегію зловмисника і визначити перелік засобів за допомогою яких можуть бути проведені будь-які нелегітимні дії проти інформаційних, та апаратних ресурсів мережевої інфраструктури, яка захищається. Конкретна реалізація HPot може являти собою як спеціальний виділений сервер (*фізично або його програмну емуляцію*), так і окремий мережевий сервіс, головне завдання якого – спробувати привернути увагу потенційних кіберзлочинців.
В контексті вищезазначеного слід підкреслити, що HPot є ресурс, який без будь-якого впливу на нього сам, практично, нічого не робить. Фактично HPot збирає певну кількість інформації, після аналізу якої їм формується відповідна статистика щодо методів і способів, якими користуються кіберзлочинці, а також визначається присутність роботи будь-яких нових (*невідомих раніше*) рішень, які згодом можуть бути застосовані при проведенні справжньої атаки. Наприклад, веб-сервер, який не має імені та фактично нікому не відомий, на практиці, не повинен мати і користувачів, що «заходять» на нього. Тому логічно вважати, що всі користувачі, які намагаються все ж таки на нього проникнути, можуть розглядатися, як потенційні порушники. В цьому випадку даний сервер - пастка буде збирати інформацію про характер поведінки цих користувачів (*частота відвідувань, їх IP-адреси, час очікування та ін.*), та про їх способи впливу на неіснуючий сервер. Після аналізу всієї отриманої інформації фахівці, які

обслуговують цю пастку, в певному сенсі повинні скорегувати алгоритм роботи аватару HPot, або іншими словами - модифікувати відповідні поведінкові шаблони так, щоб реакції пастки стали більш адекватні поточним умовам мережевої активності [4]. В цьому сенсі, в разі використання HPot з сильною взаємодією [1], буде вкрай корисно визначення загальної стратегії захисту, яка передбачає більш складні сценарії мережевої «гри» (*наприклад, каскадування HPot та/або непомітне розміщення і активація відповідного програмного "жучка" (cookie, що передані через браузер) на комп'ютері зловмисника та ін.*).

Особливості синтезу профілів мережевої активності вузлів, які захищаються за рахунок впровадження відповідних HPot, розглянемо на прикладі файлового серверу, що розміщується в демілітаризованій зоні за першим (зовнішнім) корпоративним MME. Аналізуючи типові риси роботи такого файлового серверу, можна визначити наступне (Рис. 1(а)):

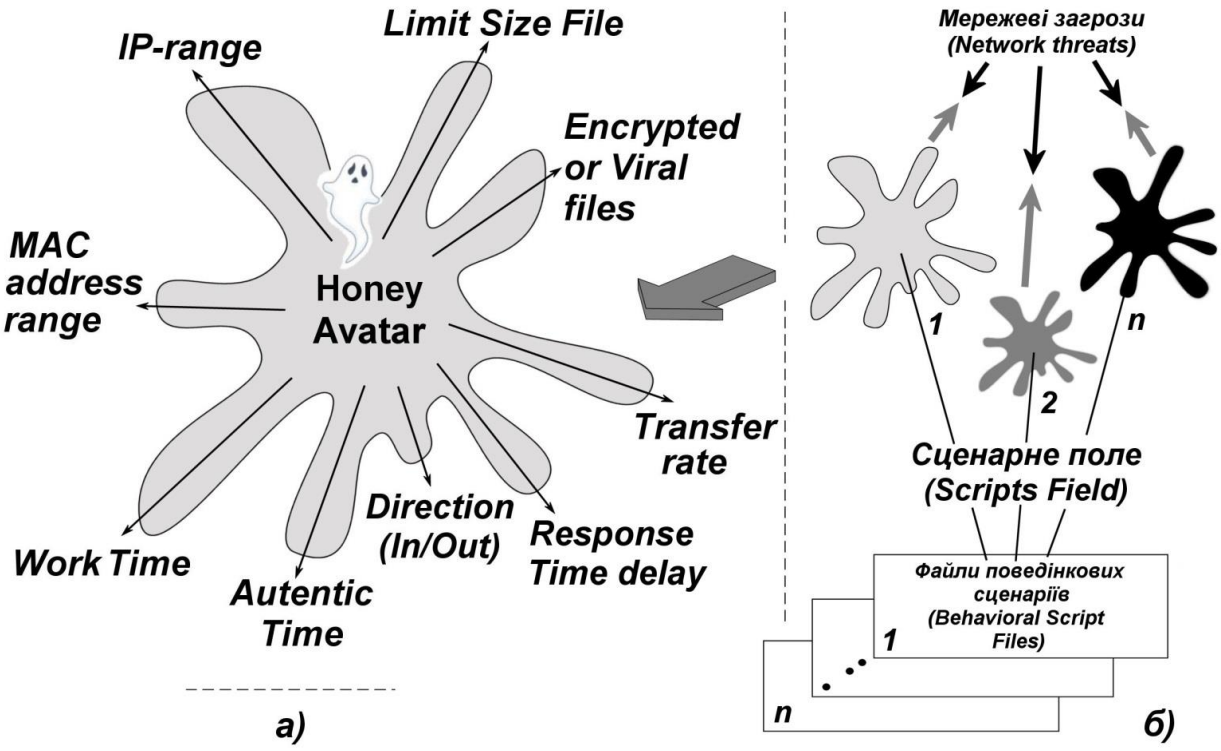

Рис. 1 – Принцип використання поведінкових профілів аватару HPot

- з ним, потенційно, можуть взаємодіяти, як зовнішні користувачі, так і користувачі з будь-якого внутрішнього сегменту локальної мережі (в залежності від їх повноважень). В даному випадку адміністрування доступу до інформаційних ресурсів серверу можливо здійснювати за рахунок управління відповідним адресним простором для IP та MAC адресів взаємодіючих абонентів («*IP range*» та «*MAC address range*»);

- обмеження розміру файлів (як скачуваних, так і тих що записуються/оновлюються на сервері), визначається функцією/правилом «*Limit size file*»;

- швидкість передачі даних з серверу можна регулювати відповідними значеннями функції/правила «*Transfer rate*»;

- затримка часу «відповіді» серверу (аналог функції уповільнення мережевих з'єднань, наприклад, як в HPot «*Tarpit*» (буде розглянуто нижче)), визначається функцією/правилом «*Response Time delay*»;

- дискретне управління можливістю зчитування-запису даних, всіма групами користувачів, визначається відповідними правилами «*Direction – In/Out*»;

- параметр правила «*Autentic Time*» дозволяє регламентувати час проходження процедури зовнішнього підключення (а саме підтвердження повноважень) для незареєстрованих/зареєстрованих користувачів;

- параметр правила «*Time Work*» дозволяє дискретно змінювати час роботи серверу для певних (або всіх) груп користувачів, що забезпечує можливість відтворювати враження спостереження перебігу інтенсивних бізнес процесів або навпаки, існування деяких технологічних пауз.

В цілому, за результатами аналізу характерних рис, що притаманні роботи кожного окремого файлового серверу, можна скласти відповідний профіль його мережевої активності. Узагальнення основних показників кожного профілю, дозволяє синтезувати відповідний аватар для його HPot (Рис. 1(а)), що забезпечить можливість імітувати роботу серверу в найбільш типових умовах мережевого оточення, та впливу актуальних (*або визначених*) мережевих загроз.

Сукупність характерних умов роботи серверу та певних ознак нелегітимного зовнішнього впливу на нього, формують відповідне сценарне поле (*Script Field*), в межах якого саме і діє даний HPot. Таким чином, чим ширше сценарне поле, тим більше можливостей у Honeypot протистояти потенційним загрозам, і тим самим більш ефективніше забезпечувати «прикриття» справжнього серверу [4]. Набір відповідних аватарів HPot, формалізується у вигляді файлів поведінкових сценаріїв («*Behavioral Script Files*», Рис.1(б)), що надає можливостей постійно розширювати спектр протидії (або моніторингу) новим загрозам, та адаптувати окремі характеристики створеної пастки під конкретну ситуацію (на відміну від випадку використання системи HPot *Specter* (*коротко буде розглянуто нижче*), яка реалізована за принципом «як є», де у її користувача немає можливості змінювати вже існуючи сценарії).

Важливо підкреслити, що створені поведінкові аватари HPot можуть мати однаковий склад параметрів, які імітуються, але відрізнятися один від одного інтенсивністю проявив кожного з них (*наприклад, аватари сценаріїв №1 та № 2 на рис.1(б) мають однакову конфігурацію, але різну довжину пліч (інтенсивність) відповідних реакцій*). Також можливо створення суттєво відмінного від інших аватару, якій має принципові відмінності, що надає йому можливостей протидіяти конкретному типу загроз (аватар «n» на Рис. 1(б)). В цьому разі поведінковим аватаром можуть підтримуватися/імітуватися, якісь дуже нетипові можливості, що значно ускладнюють доступ до «цінної» інформації яка зберігається на даному вузлі. Так наприклад, для умов файл-серверу пастки такими перешкодами можуть бути наступні (функція «*Encrypted or Viral Files*» на Рис. 1(а)):

- впровадження механізмів шифрування даних;
- впровадження механізмів багаторівневого (вкладеного) архівування даних;
- розміщення файлів з навмисно інфікованим вмістом та ін.

Зворотною стороною розвиненого сценарного поля HPot, є необхідність епізодичного аудиту його log-файлів і корекція (*т.з. тонка настройка*) файлів поведінкових скриптів. Хоча і цю рутинну процедуру можна в певної мірі автоматизувати, особливо в частині програмованих, епізодичних змін деяких робочих параметрів серверу-пастки (наприклад, зміна параметрів «*Time Work*», «*Transfer rate*» або «*Limit size file*», на рис. 5.1(а)).

Слід зазначити, що аналіз типових профілів мережевої активності для найбільш характерних об'єктів мережевої інфраструктури і подальший синтез відповідних поведінкових аватарів, необхідно проводити для кожного окремого випадку: - типу мережевих вузлів чи цілих мережевих структур (*в т.ч. і окремих мережевих сегментів*).

Так наприклад, у разі створення поведінкового аватару для цілей захисту справжнього поштового серверу, потрібно буде враховувати такі особливості, як:

- необхідність роботи з протоколами (SMTP, POP3 та IMAP);
- підтримка роботи «дозволеного» та «забороненого» списків повідомлень;
- підтримка можливості автоматичної екстракції електронних адрес з отриманого листа, та їх наступне переміщення до списку «заборонених» адресатів;
- оцінка скважністі розсилок з однієї адреси/домену;
- відслідковування розміру отриманих повідомлень і т.і.

Відповідно, врахування індивідуальних рис та ознак для кожного окремого випадку, буде в значної мірі модифікувати склад та взаємовідносини всіх складових аватару (Рис. 1(а)).

2.1 Класифікація Honeypot

В цілому HPot можна класифікувати за багатьма параметрами [5]. До найбільш принципових параметрів слід віднести наступні:

1) Характеристики процесу установки і первинних настроювань HPot. В цьому сенсі, чим більший перелік можливостей підтримує конкретний HPot, тим більш складним є і даний параметр (*особливо складно в умовах розгортання HoneyNet*);
2) Складність використання та поточної підтримки (*наприклад, частота залучення адміністратора для коригування параметрів роботи пастки та аудиту лог-файлів, частота оновлень ПЗ і т.і.*). Як і за першим параметром, чим ширше функціональність HPot, тим складніше його використання, і тим більше часу та зусиль вимагає його налагодження та підтримка;
3) Ступень взаємодії пастки з потенційним зловмисником. Очевидно, що чим більш щільна взаємодія предбачається між HPot та потенційним зловмисником, то тим більша і ймовірність помилки на кожному з етапів роботи створеної пастки. За цім параметром слід розрізняти:
   - - слабкої взаємодії;
   - - середньої взаємодії;
   - - сильної взаємодії. У більшості випадків такий HPot розташовується в контрольованому середовищі (*наприклад, після 1-го (вхідного) MME [2])*. В цілому, одного разу правильно встановлений, ретельно налаштований, та періодично перевіряєемий HPot сильного взаємодії, може надати таку інформацію, та дозволити такий спектр можливої активної протидії (в певному сенсі - гри), яку не здатен дати жоден з інших, більш простих, типів пасток. Як наслідок, рівень компетенцій фахівців, що встановлюють та обслуговують відповідній тип HPot, повинні підтримуватися на досить високому рівні;
4) Забезпечуємий рівень імітації. Даний параметр передбачає 3 можливих стана:
   - Простий, що характеризується обмеженою функціональністю імітованого сервісу (*наприклад, тільки відображення вітального повідомлення при зовнішньому з'єднанні*);
   - Середній/вибірковий, що підтримує досить докладну імітацію визначе*ного (окремого*) сервісу, або параметрів мережевої активності вузлу/мережі;
   - Високий - передбачає реалізацію всіх функціональних можливостей імітованого сервісу та/або вузлів мережі. Забезпечує підтримки пулу сценарних аватарів зворотної поведінки пастки при її реакції на спроби проведення мережевих атак;
5) Ступень потенційного ризику в разі компрометації HPot. Загальне правило: - з розширенням функціональних можливостей пастки, зростає вірогідність того, що вона може бути використана для атаки інших систем та/або сервісів. Даний параметр передбачає 3 можливих стана:
   - Низький – можлива атаку тільки проти окремого імітованого сервісу;
   - Середній – притаманний для HPot, що одночасно імітують кілька сервісів;
   - Високий – притаманний для HPot з сильною взаємодією;
6) Обсяг контрольованих параметрів мережевої активності. Найпростішим варіантом є HPot з імітацією окремого системного сервісу, а найбільш інформативним є HPot сильної взаємодії, що реалізує розширений збір всієї потрібної інформації;
7) Забезпечуємий рівень протоколювання мережевої активності (*глибина аудиторського сліду*). Даний параметр передбачае 3 можливих стана:
   - Слабке протоколювання (*зазвичай це HPot слабкої взаємодії, де фіксуються тільки IP-адреса і дані, які надходять зі сторони потенційного зловмисника*);
   - Середнє (*або вибіркове*) протоколювання (*фіксує деякі додаткові дані, наприклад, час приходу даних, ідентифікатори взаємодій і т.і.*);
   - Розширене протоколювання (*зазвичай це HPot сильної взаємодії, де реєструються всі події при взаємодії пастки із зовнішнім оточенням*).

3 Основні можливості відомих мережевих пасток

Всі існуючи HPot можна умовно поділити на 2 категорії - відкриті та комерційні [6,7]. До 1-ої категорії слід віднести такі програмні рішення, як: *Honeyd, Jackpot, BackOfficer Friendly* та ін. Характерними представниками комерційних продуктів є*: ManTrap, KFSensor, Specter* та ін. Коротко розглянемо характерні можливості декількох відкритих HPot.

3.1 Honeyd. Розроблений у 2002 році Нільсом Провосом (*Niels Provos*). Є *Open Source* рішенням для Unix-платформ. Створювався як виробничий HPot, тобто його імітовані сервіси, більшим чином, спрямовані для виявлення атак та несанкціонованої мережевої активності. Дозволяє створювати віртуальні хости в мережі (*використовується вільний простір IP-адрес*). Для опису віртуальної пастки використовується відносно простий конфігураційний файл. Цій HPot підтримує можливість власної внутрішньої установки (наприклад, додавання імітованих сервісів), та може імітувати різні операційні системи (ОС) на рівні мережевих протоколів. Імітація роботи сервісів досягається шляхом перекомутації з'єднань на робочі сервіси або використанням заздалегідь синтезованих поведінкових сценаріїв, які можна модифікувати та додавати нові. Для імітації роботи сервісів використовується відповідна база даних (*наприклад, характеристики протоколів різних ОС*). Це рішення дозволяє зробити імітацію цілої мережі, тобто створені HPot (хости-пастки) можна об'єднати у *Virtual LAN*. Таким чином, задавши потрібну топологію мережі, схему маршрутизації та визначивши припустимий відсоток втрат пакетів, можна забезпечити імітування реальної робочої мережі (*або її окремого вузлу/вузлів*). Вкрай вдалу адаптацію Honeyd для роботи з ОС сімейства Windows запропонував Майкл Девіс (*Michael Davis*): - від всіх Windows-подібних реалізацій до Unix-систем та маршрутизаторів. В цілому, Honeyd імітує систему не тільки на прикладному рівні, а також на рівні IP-стека, що надає ще більший рівень обміну інформацією зі зловмисником (або ботом-розвідником), завдяки чому цей HPot можна віднести до виду пасток середньої взаємодії.

3.2 Jackpot. Цей HPot є кросплатформним додатком (на мові Java), що являє собою імітацію поштового серверу. Розробником цієї системи є Джек Клів (*Jack Cleave*). Так як сервер з розгорнутим на ньому HPot не оголошується як загальнодоступний, то виявити поштовий сервер можна тільки при скануванні мережі (наприклад, з допомогою Nmap). В наслідок цього вся вхідна кореспонденція розглядається, як потенційний спам або, як тестові листи спамерів, які перевіряють його працездатність. В разі класифікації отриманих листів, як спам, вони далі не пересилаються. При цьому, адреси відправників, текст листів та інша (доступна) інформація про хости, з яких була проведена розсилка, зберігаються в базі даних цього HPot (*для інформування адміністратора хосту, з якого була здійснена спам розсилка*). В цілому лист визначається, як спам за наступними правилами:

- кожний наступний лист надходить через короткий проміжок часу від попереднього;
- адреса відправника є в «забороненому» списку адрес (т.з «*Blacklist File*»);
- вміст отриманого листа містить посилання на «заборонений» список адрес;
- у отриманому листі зазначено велику кількість одержувачів (адресатів).

Важливо підкресліти, що дана пастка підтримує можливість уповільнення прийому даних (функція *Tarpit*), що може досить ефективно використовуватися для організації «дрібних» неприємностей потенційному спаммеру. Як наслідок, через прикру «завантаженість каналу зв'язку» спамер розішле відчутно меншу кількість спамерських оголошень. Даний HPot має відносно прості настройки і дозволяє емулювати різні типи поштових серверів. Більш того, є можливість віддаленого адміністрування системи з використанням web-інтерфейсу, а зібрана статистика видається у форматі HTML. В якості певних недоліків, слід мати на увазі те, що при роботі не на ОС Windows, можуть виникати деякі невідповідності.

3.3 Back Officer Friendly (BOF). BOF - один з найпростіших HPot, якій може працювати під ОС Unix та Windows. Його перший реліз був представлен ще в 1998 році фахівцями з компанії *NFR Security Inc.* Варто зазначити, що певна частина спеціалістів з питань ІБ не вважають BOF справжнім HPot, однак, виходячи з його основних функціональних можливостей (*утиліта управління віддаленими комп'ютерами*) це рішення можно класифікувати, як

HPot слабкої взаємодії. Так наприклад, при виборі режиму роботи «*Fake Replies*» (*генерування помилкових відповідей*) ця утиліта використовує відповідні інтерактивні сценарії для полегшеної емуляції поточної активності мережевих сервісів. В межах реалізації функціоналу «*Fake Replies*», при фіксуванні нового з'єднання BOF інформує абонента відповідним повідомленням (*із збереженням IP-адреси, з якої надійшов цій запит*) про недоступність даного сервісу, а через заданий час повідомляє його про втрату з'єднання. Таким чином забезпечується моніторинг мережевих подій та підтримка протоколу взаємодії.

В якості недоліків даного HPot слід зазначити відсутність: – детектування «прихованого» сканування; – збереження системи в файл; – модифікації поведінкових сценаріїв; – передачі службових повідомлень по e-mail. Таким чином, за сукупність своїх можливостей та недоліків, дане рішення, в певній мірі, можна вважати ефективною пасткою лише на початку тривалого мережевого протистояння (*фактично, є засобом раннього попередження про підготовку до вторгнення*).

3.4 LaBrea Tarpit (неофіційна назва «липкий» Honeypot). Це рішення (створено Томом Лістоном) вивчає своє близьке мережеве оточення, визначає вільні IP-адреса та створює віртуальні хости, використовуючи для цього саме ці адреси. При спробах встановити з'єднання з подібною пасткою вона припиняє з'єднання, однак не розриває його. Це призводить до сканування мережі, де створені подібні віртуальні хости. Пастка може регулювати темп надходження даних по з'єднанню, оголошуючи число байтів, які вона «спроможна» прийняти в поточний момент часу. Таким чином, відправник (*потенційний зловмисник*) потрапляє в штучно створені умови, будучи вимушеним постійно адаптуватися під заявлені характеристики швидкості прийому даних зі сторони HPot. При цьому перевірка закритого вікна TCP може тривати досить тривалий період (*наприклад, поки додаток, який використовує дане з'єднання, не завершить свою роботу*). Таким чином, потенційний зловмисник потрапляє в неконтрольовану для нього ситуацію уповільнення мережевих з'єднань, що надає можливість стороні, яка захищається, виграти певний час на підготовку більш якісного захисту. В цілому цей HPot може значно уповільнити та відтягнути атаку, але не може завадити потенційним хакерам знайти спосіб щодо його нейтралізації.

Характерними представниками відомих комерційних рішень є: *ManTrap, KFSensor, Specter* та ін. Коротко розглянемо основні властивості деяких з них.

3.5 ManTrap. Цей HPot сильної взаємодії від компанії *Recourse Technologies*, котрий крім функцій пастки додатково синтезує добре контрольовану ОС, з якою взаємодіє потенційний порушник периметру безпеки. Більш того, це рішення, в межах однієї фізичній платформи, здатне утворювати контрольоване віртуальне оточення/середовище, з якого атакуючому практично дуже складно «вийти» для компрометації справжньої системи. Таким чином створюються сукупність "пасток", де кожна з них – це повноцінна функціональна ОС, яка має всі можливості, що і справжня система. При цьому передбачена функція настройки кожної окремої "пастки", як реальної фізичної ОС (*наприклад, можна створювати користувачів або запускати процеси і т.і.*). В цілому, використовуючи один комп'ютер, може бути створено до 4-х різних HPot сильної взаємодії. В якості функціональних обмежень ManTrap варто зазначити те, що це рішення підтримує лише деякі ОС, а сам HPot може функціонувати тільки на комп'ютері з ОС Solaris (з використовує особливих параметрів установки). По-друге, в силу того, що цей HPot використовує технологію "віддзеркалювання", то і основа всіх віртуальних ОС – тільки одна.

3.6 KFSensor. Цей HPot від компанії *KeyFocus* був створений для використання на системах під управлінням ОС Windows, дозволяє виявляти нелегітимні дії, за рахунок імітації вразливих сервісів ОС-жертви, та за сукупністю своїх можливостей є пасткою середньої взаємодії. Дане рішення підтримує наступні можливості: - віддалене адміністрування (*за допомогою механізмів шифрування і автентифікації*); - сумісність з IDS *Snort*; - емуляція мережевих Windows-протоколів; - має зручний користувальницький інтерфейс. Робота HPot полягає у прослуховуванні певного простору TCP/UDP-портів, а вразі зовнішньому підключення до них пастка ініціює відповідний банер (*зміст котрих можна модифікувати*) запрошення для

кожного імітованого сервісу і розриває з'єднання. В залежності від налаштувань HPot може перекомутовивати з'єднання з порту імітованого сервісу, на реально діючий сервіс іншого комп'ютера, що відбувається непомітно для зовнішнього абонента. Важливою якістю даного HPot є те, що він підтримує базу даних сигнатур, які засновані на складанні характерних ознак мережевих атак, аналогічних правилам IDS *Snort* (*можуть бути імпортовані із Snort*). За рахунок підтримки цього функціоналу, відбувається не тільки виявлення та фіксації активності мережевого зловмисника, а й забезпечується можливість створення власних скриптів відповідей та поведінки, і як наслідок, збільшення бази даних сигнатур мережевих атак. В сукупності все це надає можливість змоделювати, яку саме вразливість намагався використовувати зловмисник для проникнення в систему, що захищається. Крім того, в *KFSensor* реалізована можливість передачі повідомлень про зафіксовані мережеві інциденти по електронній пошті, що дозволяє підтримувати віддалене адміністрування та скоротити час інформування обслуговуючого персоналу, в разі виникнення необхідності оперативного втручання в перетин подій. Однак, на жаль, цей HPot не визначає прихованого сканування, та не може імітувати стек TCP/IP- протоколів.

3.7 Specter. Цей HPot від компанії *NetSec*, встановлюється в систему та імітує набір мережевих сервісів (з якими зловмисник взаємодіє), але при цьому зловмиснику не надається доступ до реальної ОС, а спект його дій обмежений передбаченою функціональністю пастки. Для того щоб ускладнити процес ідентифікації пастки для цього HPot можна призначити власне доменне ім'я, адресу, змінити банери сервісів що імітуються (*на більш характерні для кожного окремого випадку*), а також інші специфічні характеристики, що надає додаткової аргументації зловмиснику, що він таки має справу зі справжнім ресурсом. Дане рішення підтримує конфігурування потрібного рівня захищеності імітованого сервісу. Так наприклад, при імітації слабо захищеного файлового серверу, можна реалізувати можливість зовнішнього підключення, використовуючи стандартний вхід для незареєстрованих користувачів, і таким чином дозволити потенційному зловмиснику завантажити заздалегідь підроблений файл. І навпаки, в разі забезпечення високого рівня захисту сервісу, підключення до серверу-пастки може дуже ускладнити, наприклад заборонити підключення з певних IP-адресів. Корисними властивостями *Specter* є те, що він підтримує передачу службових повідомлень HPot на віддалений сервер, та має механізм передачі повідомлень по e-mail або телефонному каналу зв’язку. Однак у користувача цього HPot немає можливості додавати індивідуальні імітовані сервіси (*розширювати поведінку аватару*) або змінювати вже існуючи сценарії. Крім того, сервіси що імітуються працюють тільки з TCP-протоколом, та не підтримують UDP. Також, даний HPot є більш вимогливий до ресурсів, однак і його можливості декілька ширші порівняно з аналогами. В цілому, за сукупністю своїх властивостей *Specter* краще за всього використовувати, як систему раннього попередження про ведення мережевої розвідки або початок проведення мережевих атак.

Як випливає з матеріалів проведеного короткого огляду існуючих HPot, в незалежності від ступеня комерціалізації того чи іншого рішення, їх базовий функціонал практично завжди забезпечує імітацію основних мережевих сервісів і логирование (*з різним ступенем деталізації*) поточної мережевої активності. Таким чином, в основі практично всіх рішень є можливість раннього детектування ознак підготовки мережевої атаки або вторгнення.

4 Висновки

1. Надано огляд особливостей використання різних реалізацій програмних HPot, та визначено основні класифікаційні ознаки відомих рішень. Розглянути особливості первинних налаштувань та умов функціонування декількох відповідних комерційних засобів. За сукупністю результатів аналізу визначеної проблематики підкреслено, що основні переваги даної технології полягають в їх гнучкості та масштабованості. Можна стверджувати, що на даний час поки все ще немає досконалих методик ідентифікації та швидкої компрометації мережевих пасток. Проте, тактика мережевої розвідки і методи здійснення атак постійно прогресують,

тому забезпечення оперативної, та адаптивної протидії новим мережевим загрозам слід вважати одним із пріоритетних напрямків роботи для фахівців з питань ІБ.

2. Архітектура існуючих пасток, в цілому, достатньо добре відома і тому, є потенційно вразливою. Однак, можна стверджувати, що наділяючи пастки більш варіативним сценарним контекстом та скорочуючи час мережевої експозиції можливо підтримувати їх потенціал в досить паритетному стані. Ці обидва напряму потребують більш щільної уваги (*докладний аналіз даних log-файлів і корегування алгоритмів роботи «мережевого аватару»*) зі сторони персоналу, та вимагають постійної підтримки його професійних компетенцій. За результатами аналізу можливостей відомих HPot та узагальнення профілів мережевої активності вузла типу файл-сервер, розглянуто особливості синтезу відповідних поведінкових профілів для корегування роботи програмного аватару відповідної пастки.

3. Систематизація правил роботи мережевого аватару кожної окремої пастки (*як сукупності користувальницьких поведінкових алгоритмів*) та періодична корекція наявних поведінкових профілів, є завданням, що важко формалізувати (*через різноманіття особливостей функціонування як всієї мережі, так і її окремих вузлів*). В цьому сенсі надлишкова уніфікація поведінкових профілів HPot (*для кожного типу вузлів*) в певній мірі може полегшити зловмиснику ідентифікацію діючої пастки. Тому наявність базового набору поведінкових профілів HPot слід розглядати, не більше, як основу для подальшої модифікації аватару під специфіку завдань, топологію та інші особливості кожної мережевої структури [4].

4. Впровадження технології пасток не підміняє інших механізмів мережевої безпеки, а лише ефективно розширює наявний арсенал засобів мережевого моніторингу та протидії новим загрозам (*перш за все, як інструмент попередньої розвідки та швидкого реагування*). Тому шлях комплексування мережевих пасток з іншими рішеннями ІБ, є найбільш збалансованим напрямом подальшого підвищення загального рівня безпеки мережевих ресурсів.

Посилання

[1] Рузудженк, С., Погоріла, К., Кохановська, Т., & Малахов, С. (2020). Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. Комп'ютерні науки та кібербезпека, (4), 22-29. Retrieved із https://periodicals.karazin.ua/cscs/article/view/15751

[2] Безопасная сеть вашей компании / Джон Маллери, Джейсон Занн и др.; пер. с англ. Е. Линдеманн. – М.: НТ Пресс, 2007. – 640 с.

[3] Ріпний О.С., Дьяченко О.О., Малахов С.В. // Особливості функціонування систем IDS та IPS при реалізації спроб несанкціонованого доступу до корпоративних ресурсів. Матеріали IX міжнародній НТК. 11-12.04.2019. – Х.: НТУ "ХПІ". – 2019. – С.95.

[4] Кохановська Т. А. Дослідження можливостей технології Honeypot : Пояснювальна записка до дипломної роботи бакалавра: напрям підготовки 125 – Кібербезпека / Т. А. Кохановська; Харківський національний університет імені В. Н. Каразіна. – Харків: [Б. В.], 2020. – 45 с.

[5] Технология Honeypot, Часть 2: Классификация Honeypot. DOI: https://www.securitylab.ru/analytics/275775.php (дата звернення: 2.10.2019)

[6] Технология Honeypot, Часть 3: Назначение Honeypot. DOI: https://www.securitylab.ru/contest/283103.php (дата звернення: 24.11.2019)

[7] Красоткин А. Черный лед // СНІР. – 2003. - №7. – *С. 98-103.*

Reviewer: Oleksandr Oksiiuk, Doctor of Sciences (Eng.), Full Prof., Taras Shevchenko National University of Kiev 81 Lomonosova St., Kyiv, 03189, Ukraine. E-mail: o.oksiuk@gmail.com

Received on March 2020.

Authors:

Tetiana Kokhanovska, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: tanya.koh99@gmail.com

Oleksii Nariezhnii, Ph.D., Associate Professor, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: o.nariezhnii@karazin.ua

Alexandr Dyachenko, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: diachenko4@gmail.com

Researching the possibilities of Honeypot technology.

Abstract. The role and main tasks of various network traps (Honeypot) in the construction of integrated security systems are defined. Basic classification signs and features of the primary tuning of a few commercial facilities software solutions. It is concluded that the

main advantages of Honeypot technology, among other things, are their flexibility and scalability. It is emphasized that at present there are no perfect methods of identification and rapid compromise of network traps. Attention is drawn to the fact that network intelligence tactics and methods of network attacks are constantly progressing. Given this fact, the ongoing audit of HP data and prompt response to identified network incidents is one of the main areas of work for staff on compliance with corporate information security policy requirements. It is noted that the architecture of various traps, in general, is quite well known and therefore potentially vulnerable. Therefore, by providing traps with a more flexible (variable) scenario context and reducing the exposure time, it is possible to maintain their protective potential in the parity enough state. Both of these direction require closer attention (detailed analysis of log-files data and adjustment of behavioral avatar algorithms for the created trap) on the part of staff, and require constant support of them professional competencies. Based on the results of reviewing the capabilities of existing Honeypots and generalizing the typical features of network activity of the most characteristic nodes (in this case the file server), the features of synthesis of the corresponding behavioral profiles (avatars) are considered. It is claim that systematization of avatar rules Honeypot (as a set of behavioral algorithms) and timely correction of existing databases of behavioral profiles is a task that is difficult to formalize. This is caused to the potential variety of network activity options that are specific to each network and the individual settings of existing network nodes. In this sense, excessive unification (narrowing of the possible field of behavioral reactions) of behavioral profiles Honeypot can greatly facilitate the attacker to monitor and subsequently identify the trap created. Therefore, the formation of a basic set of relevant network avatars should be considered as a basis for its further modification under a special task, topology and other features of each individual IT structure (or features of their individual elements). It is emphasized that the introduction of trap technology does not replace other security technologies and tools, but only effectively expands the existing arsenal of countering new security threats (primarily as a tool for operational intelligence and rapid response). Therefore, the way to integrate net-traps with other security solutions is the most balanced way to further improve the overall security of network resources.

Keywords: Honeypot; Intrusion; Informational security; LAN; Firewall; IDS; IPS.

Рецензент: Александр Оксиюк, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, ул. Ломоносова 81, Киев, 03189 Украина. E-mail: o.oksiuk@gmail.com

Поступила: Март 2020.

Авторы:

Татьяна Кохановская, студентка факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: kate7smith12@gmail.com

Алексей Нарежний, к.т.н., доцент, каф. безопасности информационных систем и технологий, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: o.nariezhnii@karazin.ua

Александр Дьяченко, студент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина. E-mail: diachenko4@gmail.com

Исследование возможностей технологии Honeypot.

Аннотация. Определена роль и основные задачи различных разновидностей сетевых ловушек (Honeypot) при построении интегрированных систем безопасности. Рассмотрены основные классификационные признаки и особенности первичных настроек нескольких коммерческих средств. Сделан вывод, что основные преимущества технологии Honeypot, среди прочего, заключаются в их гибкости и масштабируемости. Подчеркнуто, что в настоящее время пока еще нет совершенных методик идентификации и быстрой компрометации сетевых ловушек. Обращено внимание на то, что тактика сетевой разведки и методы осуществления сетевых атак постоянно развиваются. Учитывая этот факт, постоянный аудит данных Honeypot и оперативная реакция на выявленные сетевые инциденты и коллизии, является одним из главных направлений работы для специалистов по вопросам обеспечения требований корпоративной политики информационной безопасности. Отмечено, что архитектура разных ловушек, в целом, достаточно хорошо известна и поэтому является потенциально уязвимой. Поэтому, наделяя ловушки более гибким (вариативным) сценарным контекстом и сокращая время сетевой экспозиции, можно поддерживать их защитный потенциал в достаточно паритетном состоянии. Эти оба направления требуют более пристального внимания (подробный анализ данных log-файлов и корректировка алгоритмов работы поведенческого аватара ловушки) со стороны персонала и постоянной поддержки их профессиональных компетенций. По результатам обзора возможностей существующих Honeypot и обобщения характерных признаков сетевой активности типовых узлов (в данном случае файлового сервера), рассмотрены особенности синтеза соответствующих поведенческих профилей (аватаров) для коррекции работы программных ловушек. Утверждается, что систематизация правил работы аватара для сетевой ловушки (как совокупности пользовательских поведенческих алгоритмов) и своевременная коррекция имеющихся поведенческих профилей, является задачей, которая трудно формализуется. Это обусловлено потенциальным многообразием вариантов сетевой активности, характерных для каждой конкретной сети и настроек имеющихся сетевых узлов. В этом смысле избыточная унификация (сужение возможного поля поведенческих реакций) поведенческих профилей Honeypot, в значительной степени может облегчить злоумышленнику проведения мониторинга и последующей идентификации созданной ловушки. Поэтому формирования базового набора соответствующих сетевых аватаров следует рассматривать, не более чем, как основу для ее дальнейшей модификации под специфику задач, топологию и другие особенности каждой отдельной IT-структуры (или особенности их отдельных элементов). Подчеркнуто, что внедрение технологии ловушек не подменяет собой других технологий и инструментов безопасности, а только эффективно расширяет имеющийся арсенал противодействия новым угрозам безопасности (прежде всего, как инструмент быстрого реагирования). Поэтому путь интеграции Honeypot с другими, уже развернутыми решениями ИБ, является наиболее сбалансированным направлением для дальнейшего повышения общего уровня безопасности сетевых ресурсов.

Ключевые слова: Honeypot; вторжение; информационная безопасность; ЛВС; межсетевой экран; IDS; IPS.