УДК 004.056.5 DOI: 10.26565/2519-2310-2019-4-03

ОСОБЛИВОСТІ ЗАХИСТУ КОРПОРАТИВНИХ РЕСУРСІВ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ HONEYPOT

Сабіна Рузудженк, Каріна Погоріла, Тетяна Кохановська, Сергій Малахов

Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
ruzudzhenk.jb@gmail.com, karina.pogorelka@gmail.com, tanya.koh99@gmail.com, mailgate@meta.ua

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: Листопад 2019.

Анотація: *У статті надано стислий огляд основних можливостей технології Honeypot. Розглянуті питання стосовно: - особливостей моніторингу мережевої активності на різних етапах розвитку атак/вторгнень; - розміщення датчиків системи; - процедур збору та узагальнення даних щодо мережевих подій; - варіантів модифікації інструментів захисту; - організації структури захисту тощо. Розглянуті загальні принципи роботи відповідних систем на базі відокремлених серверів та програмно емульованих мереж. Узагальнено основні недоліки даної технології. Звернено увагу на перспективність використання різноманітних рішень Honeypot для цілей розширення потенціалу вже розгорнутих засобів забезпечення інформаційної безпеки (ІБ).*

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

1 Вступ

У сучасному світі інформаційних технологій кожен Інтернет користувач та локальна обчислювальна мережа, які мають підключення до Інтернет, рано чи пізно, але в будь-якому випадку, неминуче стикаються з проблемою зовнішніх кібератак. Враховуючи цей факт, як аксіому, можна зробити висновок, що відповідні інформаційні і апаратні ресурси Інтернет користувачів та локальних обчислювальних мереж (ЛОМ), що взаємодіють з Інтернет, обов'язково повинні бути спроможні парирувати відповідні загрози. Саме тому, на постійній основі, необхідно забезпечувати комплексний моніторинг поточної мережевої активності, особливо в частині аналізу змісту, характеру та інтенсивності трансграничного трафіку. В першу чергу це стосується аналізу трафіку в межах спеціально передбачених демілітаризованих зон, або 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 мережевої активності та виявлення ознак підготовки майбутнього кіберзлочини, є використання можливостей технології Honeypot (*т.з. вузлів або мереж пасток/приманок*). Крім того потенціал Honeypot дозволяє, в буквальному сенсі, виграти час, відволікаючи мережевого зловмисника або спеціалізовану програму на виконання завідомо зайвих або хибних дій.

Аналіз джерел. Honeypot вперше з'явилися з першими комп'ютерними зловмисниками, а практика їх активного використання налічує вже більше 20 років. Роботи по їх створенню та практичному впровадженню проводилися паралельно з дослідженнями IDS та IPS [1]. Першою документальною згадкою за тематикою Honeypot, була робота Кліффорда Столла «The Cuckoo's Egg», що вийшла у 1990 році. А вже у 2000-х роках Honeypot стали досить поширеними системами, що забезпечували ефективну протидію спробам несанкціонованого проникнення до «внутрішнього» периметру безпеки комп'ютерних мереж компаній.

На сьогоднішній день актуальним напрямом використання вузлів і мереж – приманок є, наприклад, протистояння діям кіберзлочинців при парируванні розгалужених атак типу «відмова в обслуговуванні (*DDos*) при використанні різних моделей хмарних обчислень (*наприклад, PAAS або IAAS*). Застосування Honeypot полегшує збір інформації про потенційну атаку і атакуючого вже на етапах підготовки (*попередньої розвідки*) та початку «проникнення» в

відповідну систему. В цілому, Honeypot можна використовувати, як дуже ефективне доповнення до технологій виявлення та запобігання несанкціонованих вторгнень (IDS/IPS) [2,3].

Як правило, створюючи Honeypot (далі HPot) фахівці з інформаційної безпеки (ІБ) очікують від нього/неї вирішення 3-х основних завдань: 1 - отримання змістовної інформації щодо використовуваних кіберзлочинцями способів та методик проникнення до ресурсів мережі, що захищається; 2 - реєстрація моменту початку атаки (*несанкціонованого проникнення до мережі або доступу до вузла-пастки*); 3 - забезпечення виграшу часу, за рахунок переорієнтації уваги хакера з фактичних елементів і ресурсів ЛОМ на їх неіснуючі мережеві клони (*копії-пастки*). В цілому HPot, це досить гнучкий інструмент, який, залежно від умов роботи (*шлюз, вузол, сукупність вузлів, гібрид*) та кінцевих завдань (*захист від спам-ботів або система раннього попередження про мережеві інциденти тощо*), можливо застосовувати в різних іпостасях [4]. Так наприклад, це може бути програмний «емулятор» іншої системи, додаток або стандартна система/системи. Як свідчить досвід [1-2, 4-5], HPot може виконувати досить різні завдання, наприклад: - визначати початок атаки; - збирати інформацію про несанкціонований моніторинг поточної мережевої активності; - фіксувати інформацію про задіяні механізми витоку даних, служити засобом захисту від спам-ботів тощо. При цьому впровадження HPot може переслідувати діаметрально протилежні цілі, наприклад: організовувати виробничі і/або дослідні пастки, де перші зорієнтовані на питаннях захисту мережі, а другі на зборі відповідних додаткових уточнюючих відомостей [6].

Актуальність. Таким чином, розгляд питань стосовно особливостей використання HPot в сучасних умовах та можливостей їх подальшої модифікації в майбутньому (*віртуалізація процедур аналізу трафіку в визначених мережевих сегментах, адаптивне шлюзування мережевого трафіку, оперативна кластеризація HPot, врахування можливостей блокчейн тощо*), не визиває ніяких сумнівів.

2 Основна частина

Зазвичай HPot являє собою програмно-апаратний комплекс, якій складається з наступних основних компонентів: - вузол-приманка, мережевий сенсор і накопичувач даних про всю аномальну мережеву активність [7]. В якості майбутньої приманки організовується певний сервер (Рис. 1), що працює під управлінням довільної операційної системи (ОС), та настроюється на потрібний, в даних умовах, рівень безпеки (*протидії потенційному нападнику*). Ізольованість від інших ділянок (*сегментів*) ЛОМ, потенційно перешкоджає використанню вузла-приманки, як платформи для майбутніх атак на інші елементи мережі, однак, надає хакеру можливість швидко зрозуміти, що він вже на півдорозі до «успіху». Найчастіше вузлів з приманкою буває кілька. В цьому разі одні з них розраховані для протидії хакерам-початківцям, а інші – більш захищені та «тонко» налаштовані, орієнтовані на виявлення ще невідомих технік злому, які очікуються з боку більш досвідчених мережевих зловмисників.

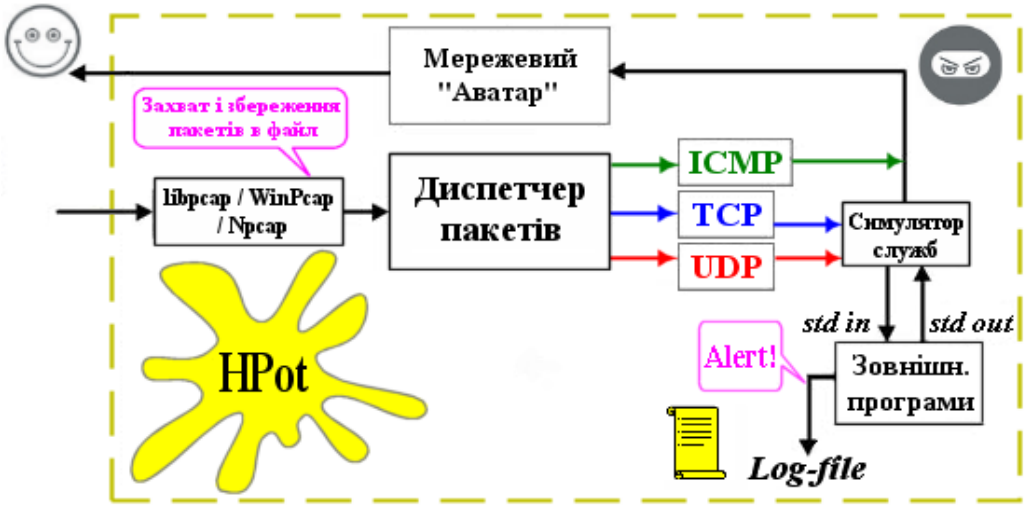

Рис. 1 – Спрощена схема Honeypot з низьким рівнем взаємодії *(варіант)*

Мережевий сенсор найчастіше реалізується на базі UNIX-подібних операційних систем (ОС), а для моніторингу поточної інформації використовується утиліта *tcpdump* або її аналоги [2]. При цьому, залежно від конфігурації мережі, що захищається, сенсор може знаходитись на одному з вузлів визначеного сегмента ЛОМ, або бути маршрутизатором, якій розташований перед приманкою. Іноді мережевий сенсор поєднується безпосередньо з самої приманкою, що істотно спрощує та здешевлює реалізацію HPot, однак, послаблює безпеку всієї системи (*захопивши управління приманкою, атакуючий швидко виявить сенсор, та нівелює всю систему*). Розміщення сенсора на одному з вузлів визначеного сегмента мережі забезпечує йому найбільшу конфіденційність *(мають на увазі труднощі з його виявлення)*. При цьому мережевий інтерфейс сенсора може і не мати власної IP-адреси, прослуховуючи трафік в т.з. «стелс-режимі». При виносі сенсору системи на маршрутизатор *(перед приманкою),* визначити чи працює на ньому мережевий сенсор, чи ні, в загальному випадку є дуже складно.

Іншим напрямом є використання програмно емульованих HPot [7]. На відміну від фізично розгорнутих на окремому сервері/вузлі систем, програмно емульовані рішення швидко відновлюються в разі їх злому, а також досить чітко обмежуються (*відокремлюються*) від «основної» ОС. Подібні рішення можуть бути створені, наприклад, за допомогою віртуальної машини або Honeyd [5].

Основна відмінність між ними полягає у різниці масштабів корпоративної обчислювальної мережі, що потребує захисту. Так наприклад, у випадку малої офісної ЛОМ не має особливого сенсу організовувати виділений сервер для цілей протоколювання підозрілих мережевих подій. В цьому разі досить буде обмежитися віртуальною системою або навіть одним віртуальним сервісом. Однак, у великих організаціях з розвиненою IT-структурою, потрібно використовувати саме виділені сервери з повністю відтвореними на них мережевими службами. При цьому, зазвичай в конфігурації таких служб навмисно допускають відповідні помилки-пастки, щоб у потенційного зловмисника обов'язково «вдався» злом системи. А як було зазначено вище, саме у цьому і полягає основна мета впровадження Honeypot – привернути увагу зловмисника та виграти у нього час, для організації ефективного парирування даного різновиду загроз ІБ.

Слід зазначити, що залежно від ступеня взаємодії зі зловмисником HPot діляться на 3 типи: - слабкої, середньої та сильної взаємодії. Основна відмінність відповідних реалізацій систем полягає в складності їх розгортання, використання і підтримки, а також в забезпечуваних рівнях імітації та протоколювання даних мережевої активності. Так, засоби слабкої взаємодії порівняно легко розгортаються та більш прості у подальшої експлуатації, але вони і менш ефективні (*с точки зору можливостей реєстрації інформації та ступеню мережевої мімікрії*). В цьому сенсі засоби систем з сильною взаємодією забезпечують більш глибокій рівень протоколювання і імітації, проте вони є і більш складними у використанні, та потребують більш високих професійних компетенцій персоналу. Крім того, впровадження такого типу HPot тягне за собою більш високий ризик їх виявлення і наступної компрометації.

В цілому, незважаючи на те, що HPot ретельно налаштовані (*в наслідок чого їх важко виявити*), при певних зусиллях та обачливості можливо виявити деякі ознаки того, що ми маємо справу саме з ними. Так наприклад, у разі використання фішингу [2], зловмисні URL–адреси часто відрізняються від легітимних ресурсів тільки однією літерою або цифрою, тому відповідна пильність зовсім не є надмірною. В цьому разі, перш за все, потрібно завжди уважно перевіряти правильність вводу відповідної URL-адреси. Крім цього, якщо «довірений» веб-сайт раптом починає запитувати облікові дані або будь-яку іншу «чутливу» інформацію, чого раніше за ним помічено не було, це також повинно насторожити.

На практиці існують достатньо прості кроки, що дозволяють уникнути можливих наслідків: - ніколи не клікати підозрілі посилання, що отримані з неперевірених або невідомих для користувача джерел; - отримане посилання більш безпечно перенабрати в адресної строчці браузеру, ніж клікати отримане посилання; - використовувати безпечні DNS сервіси [8]; - перевірити наявність сайту в переліку DBL (*реєстрі заблокованих доменів*) [9].

У разі проведення атаки, хакеру важливо мати надійні та швидкі канали зв'язку, щоб забезпечити собі можливості маневру проти спроб його відстеження. Так наприклад, в разі перебування в широкомовній мережі, для успішного маскування дій він може обмежитися клонуванням чужих IP і/або MAC-адрес [2, 9]. В цьому випадку, за умови, що ЛОМ яка атакується не має ніякого додатково обладнання, для визначення дій порушника, ідентифікувати зловмисника буде практично неможливо, хоча і тут є одне «але». Так, в разі якщо комп'ютер хакера вразлив, то HPot може непомітно для нього розмістити і активувати відповідного програмного "жучка" з усіма можливими наслідками *(наприклад cookie, що передані через браузер)*. Крім того, очікуючи атаку зловмисника, треба враховувати, що при її здійсненні він може передбачити певні захисні заходи, наприклад: використовувати ланцюжок з кількох комп'ютерів або гаджетів, а в глобальну мережу виходити з однієї з публічних точок доступу, якнайдалі від свого основного місця розташування, щоб значно ускладнити свою локацію. В любому випадку виходити в мережу по комутованому доступу для нього буде вкрай небезпечно, та скоріш за все буде впроваджено механізм каскадних *proxy*. Але і в цьому разі йому не слід цілком покладатися на можливості *proxy*, оскільки заздалегідь ніколи невідомо фактичний рівень протоколювання даних підключення на кожному з задіяних *proxy*-серверів. В цьому контексті слід зауважити, що частина безкоштовних *proxy* в дійсності є своєрідними приманками, що встановлені та підтримуються відповідними службами.

Враховуючи специфіку технології HPot для забезпечення належного рівня захисту корпоративних ресурсів (*перш за все інформаційних*) слід враховувати можливі способи обходу потенційними зловмисниками цих приманок. Так, серед іншого, з метою перешкоджання спроб їх ідентифікації, зловмисники можуть запровадити наступні дії:

- використовувати технологій анонімізації і тунелювання;
- впровадити технології мережевого аватару *(вигаданої віртуальної особистості, що ніяк не пов'язана з реальною)*;
- відмовитись або значно обмежити чисельність завантажень будь-яких файлів (в тому числі ПЗ), окрім випадків, коли вони будуть отримані з вкрай надійного, з їх точки зору, джерела.

В даний час окрім відповідних рішень технології HPot та її похідних (*Honeynet, Honeytoken, Honeyd тощо*) в різних комбінаціях активно застосовуються і інші засоби забезпечення ІБ комп'ютерних мереж такі, як Padded Cell, міжмережеві екрани, IDS, IPS, DLP тощо [2-4, 8, 10]. Останні рішення являють собою не пасивні приманки, а активно протидіючи засоби парирування, як відомих, так і ще невідомих загроз ІБ. Найбільш близьким до HPot за низькою функціональних ознак є IDS (*система виявлення вторгнень*), що протоколює всі «зовнішні» мережеві підключення до системи, в цілому, або її окремого сегменту/сегментів. Honeynet поєднує у собі декілька Honeypot-приманок, що поєднані єдиним задумом, та складають інтегровану мережу-пастку. Honeytoken є приманкою, основним завданням котрої є виявлення випадків неправомірного використання даних. В основу роботи Honeytoken положено принцип «попередити, а не запобігти». На відміну від них, Padded Cell – це своєрідний різновид приманки типу «пісочниця». Потрапляючи до неї, зловмисник істотно обмежений в можливостях завдати шкоди системі-жертві, так як він фактично розташований в ізольованому від іншої системи/процесів середовищі. На відміну від попередніх, DLP-системи, є більш інтегровані та високоінтелектуальні системи, які поєднують єдиним задумом (алгоритмом) роботу багатьох інших підсистем та засобів «активного» та «пасивного» мережевого захисту (*ті ж самі HPot, firewall. IDS та IPS*).

В цілому, пам'ятаючи про основне призначення мережевих приманок – створення максимальної ілюзії фактичного доступу до «внутрішніх» корпоративних ресурсів, приманка повинна бути спеціальним чином підготовлена. Іншими словами, вона повинна містити фальшиву інформацію, яка своїм складом і контекстом, відповідає основному профілю діяльності компанії-жертви. В такому випадку у потенційного зломщика системи, буде підтримуватися стійке враження про успішне завершення реалізованої їм атаки. При менш оптимістичному для зломщика результаті подій, використання HPot забезпечить виграш часу для сторони, що

захищається (*фахівців компанії, які відповідають за питання ІБ*), таким чином, даючи їм можливість модифікувати тактику захисту, та «втягнути» хакера в більш тривалий цикл мережевого протистояння. В принципі ця «гра», якщо і не відіб'є у хакера бажання «зламати» обрану їм мережу, то, принаймні, тільки посилить у нього враження про реальність того, що відбувається, що і потрібно отримати, в кінцевому підсумку.

3 Основні переваги та недоліки технології Honeypot

Аналіз особливостей захисту корпоративних ресурсів за допомогою використання відповідних мереж приманок, дозволяє виділити, як ряд очевидних переваг, так низку специфічних недоліків даної технології [11,12]. Так, до сильних сторін HPot слід віднести наступне:

1. *Ретельний збір змістовної інформації про мережеві події*. Засоби HPot збирають невелику кількість даних (*порядку кілька мегабайт на добу*), але, зазвичай, вони мають принципове, з точки зору аудиту ІБ, значення. Дані, які були зареєстровані HPot, найбільш ймовірно є результатами сканування, несанкціонованого дослідження (мережевою розвідкою) або ознаками атаки - тобто є інформацією, що має високий пріоритет для відповідного аналітика. Таким чином, HPot надає аудитору ІБ практично всю потрібну інформацію, причому фактично в режимі реального часу. Це спрощує аналіз мережевої активності, зменшує час реакції, та надає можливість вжити превентивні заходи щодо завчасного парирування відповідних загроз ІБ.

2. *Невимогливість до системних ресурсів*. З точки зору питань підтримки безперервності процесів забезпечення ІБ, нестача ресурсів – це ситуація, коли задіяні механізми HPot не можуть бути продовжені, тому що наявні або виділені для цього ресурси вже вичерпані. Але, в цілому, використання HPot забезпечує потрібний баланс завдань ІБ та наявних ресурсів.

Оскільки засоби Honeypot, в своєї переважної більшості, спрямовані на завдання контролю і фіксації мережевої активності в визначеному сегменті/вузлі ЛОМ, то зрозуміло, що вони зазвичай не схильні до проблем нестачі ресурсів. Це відрізняє HPot від більшості IDS (систем виявлення вторгнень), які мають певні складності при забезпеченні завдань ІБ в високошвидкісних ІТ-структурах.

3. *Очевидність практичного використання*. Існуючи засоби HPot оперативно та неодноразово підтверджують своє основне призначення, як інструменту перманентної мережевої розвідки, всякий раз, коли їх елементи піддаються нападу або неавторизованому зондуванню, підтверджуючи тім самим прояви несанкціонованої мережевої діяльності.

У будь-якому випадку HPot є досить простим і переконливим засобом підтвердження правоти твердження: - що, якщо ви параноїк, то це ще не означає, що за вашої ІТ-структурою ніхто не спостерігає. Таким чином, коли хтось раптом вирішить, що вже немає ніяких загроз, то саме HPot зможе ефективно довести зворотне та документально підтвердити, що загроза бути скомпрометованим постійно була поряд, і більш того, очікує саме на вас.

4. *Простота розгортання та подальшої експлуатації*. Порівняльна простота процедур встановлення та первинного конфігурування HPot є найбільш вагомим аргументом на користь даної технології. Для більшої об'єктивності слід зазначити, що для різних HPot існують і різні додаткові функціональні розширення *(бази сигнатур відомих атак, бази типових реакцій і т.ін.)*, але в любому випадку *(в незалежності від типу системи та місця її розгортання)* фундаментальна парадигма залишається незмінною: – якщо хтось або щось з'єднується з HPot, то це вимагає обов’язкової перевірки.

Як вже було зазначено вище, поряд з очевидними та вкрай корисними можливостями HPot, вони мають і ряд характерних недоліків, до яких слід віднести:

1. *Можливість «розкриття» (демаскування) пастки*. Можливість розкриття HPot зловмисником – в любому випадку базується на його компетенціях зі збору та узагальнення відповідної інформації, за наслідками котрої він саме і може ідентифікувати істинну сутність досліджуємого об’єкту (*за сукупністю очікуваних характеристик або особливостей мережевої поведінки*). В загальному випадку можливість компрометації HPot залежить від двох основних факторів: - кваліфікації зловмисника та коректності налаштувань самого HPot. Тому,

якщо питання селекції рівня професійної кваліфікації зловмисника виходить за рамки компетенції відповідних фахівців з питань корпоративної ІБ, то питання конфігурування та впровадження коректних налаштувань HPot, повністю залежить від відповідного персоналу.

2. *Обмежену область спостереження (контролю)*. Від самого початку Honeypot здійснюють моніторинг мережевої діяльності, яка була спрямована саме проти них. В разі, якщо дії атакуючого будуть спрямовані на інші елементи ЛОМ, HPot практично вже не буде спроможним фіксувати дану діяльність. В враховуючі цю особливість, слід постійно мати на увазі, що в разі ідентифікації зловмисником HPot (*безвідносно того, як саме він це зробив*) він може спробувати «обійти» його, та переключити свою увагу на інші – справжні елементи мережі, що захищається. В цьому випадку, для фахівців які забезпечують захист мережі, фактор часу стає критичним, тому що компрометована пастка в буквальному сенсі «вимкнена з гри» (*аналогічно ситуації коли противнику відома карта міного поля, що дає йому можливість прокласти безпечний маршрут*). Таким чином, обмежена зона контролю кожного окремого HPot, практично виключає контроль мережевих подій поза зоною його відповідальності. Як наслідок, для подолання цього ефекту необхідно комбінувати порядок розміщення датчиків HPot, тобто: - або дублювати, або каскадувати відповідні елементи HPot, що призводить до загального ускладнення відповідної системи та зростанню її вартості.

3. *Збільшення ймовірності початку таргетованих атак елементів інших IT-структур, внаслідок випадків компрометації/злому кожного HPot*. Різні HPot мають різні рівні ризику, для елементів інших мереж. Так деякі з них мають дуже невеликий ризик, в той час, як інші надають атакуючому досить широкі можливості для наступних атак (*наприклад, створення фішингових ресурсів або бот-систем для спамерів*). В цьому сенсі, існує проста думка, що чим простіше діючий HPot, то тим менший потенційний ризик його подальшого протиправного застосування.

4 Висновки

1. Основні переваги HPot, серед іншого, полягають в їх гнучкості та масштабованості. На даний час у мережевих злочинців поки все ще немає досконалих методик детектування та подолання захисних механізмів різних HPot, проте, стратегії мережевої розвідки і методи атак постійно прогресують, тому питання побудови ефективної адаптивної протидії новим мережевим загрозам є одним із найважливіших напрямів роботи відповідних фахівців.

2. Архітектура різних HPot, в цілому, достатньо добре відома і тому, потенційно, вразлива. Однак, наділяючи HPot-рішення більш складним сценарним контекстом та скорочуючи час мережевої експозиції можливо підтримувати їх потенціал в досить паритетному стані. Обидва напряму потребують більш щільної уваги відповідних фахівців (*аналіз лог-файлів і вдосконалення алгоритмів роботи «мережевого аватару» HPot*), та підтримки їх професійного реноме на досить високому рівні (*постійне навчання та вдосконалення навичок*).

3. В контексті сказаного, з великою часткою впевненості можна стверджувати, що систематизація правил роботи мережевого аватару HPot (*як сукупності користувальницьких поведінкових алгоритмів*) та синтез уніфікованих наборів відповідних поведінкових профілів для HPot, бачиться, як завдання, що важко формалізується (*в першу чергу, через різноманіття варіантів мережевої активності, що притаманна для кожної конкретної реалізації окремих мереж та визначених мережевих вузлів*).

4. Надлишкова уніфікація поведінкових профілів HPot певною мірою може полегшити потенційному мережевому зловмиснику процес моніторингу і наступної ідентифікації HPot (*за сукупністю характерних ознак*), тому формування пулу відповідних мережевих аватарів слід розглядати, не більше, як основу для її подальшої адресної підгонки (*налаштування*) під специфіку характерних завдань, топологічні та інші особливості кожної IT-структури або їх окремих елементів (вузлів).

5. HPot не підміняють собою інших механізмів безпеки, а лише ефективно розширюють наявний арсенал засобів мережевого моніторингу, та в певній мірі, протидії новим загрозам безпеки (*перш за все, як інструменту швидкого або випереджаючого реагування*). Тому

шлях інтеграції HPot з іншими, вже розгорнутими рішеннями ІБ, є найбільш збалансованим напрямом подальшого підвищення загального рівня безпеки мережевих ресурсів.

6. Honeypot є гнучким та достатньо бюджетним інструментом отримання первинної інформації для дослідження нових методик і різновидів дій мережевих зловмисників. Ретельний аналіз відповідної інформації дозволяє досить ефективно відслідковувати, як еволюцію технік мережевого нападу, так і прийомів маніпулювання мотиваціями кіберзловмисників.

Посилання

[1] Сильнов Д. С., Титов К. Е., Разработка и реализация Honeypot-ловушек сетевых служб, использующих протокол SIP, DOI: https://cyberleninka.ru/article/v/razrabotka-i-realizatsiya-honeypot-lovushki-setevyh-sluzhb-ispolzuyuschih-protokol-sip

[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] Honeypot success stories Ел.ресурс. – URL: https://www.drupal.org/docs/8/modules/honeypot/honeypot-success-stories

[5] Honeypots – University of Arizona Ел.ресурс. – URL: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic12-final/report.pdf

[6] HoneyPot для спамеров. Персональный блог Игоря Агурьянова Ел.ресурс. – URL: http://aguryanov.blogspot.com/2014/08/honeypot-for-spammer.html

[7] M. M. Rehman H., Honeypots and Routers Collecting Internet Attacks, 2015.

[8] Валерий Коржов Google Public DNS как средство защиты. Ел.ресурс. – URL: https://www.anti-malware.ru/node/2299 (дата звернення 12.12.2019)

[9] Chris Moore, Detecting ransomware with Honeypot techniques. DOI: https://ieeexplore.ieee.org/abstract/document/7600214

[10] Череватенко Д. Р., Торбеева М. В., Honeypot как средство информационной безопасности, DOI: http://ir.nmu.org.ua/bitstream/handle/123456789/1679/19.pdf?sequence=1&isAllowed=y

[11] Lance Spitzner, Honeypots: tracking hackers. Ел.ресурс. – URL: http://www.it-docs.net/ddata/792.pdf

[12] Технология Honeypot, Часть 1: Назначение Honeypot. DOI: https://www.securitylab.ru/analytics/275420.php

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 November 2019.

Authors:

Sabina Ruzudzhenk, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: ruzudzhenk.jb@gmail.com

Karina Pogorelaya, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: karina.pogorelka@gmail.com

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

Serhii Malakhov, Ph.D., Senior Research, Associate Prof. of the Department, V. N. Karazin Kharkiv National University, Ukraine.
E-mail: mailgate@meta.ua

Features of protecting corporate resources with Honeypot technology.

Abstract. The article provides a brief overview of the main features of Honeypot technology. The questions concerning are considered: - features of monitoring network activity at different stages of attack development; - placement of system sensors; - procedures for collecting and summarizing data on network events; - options for modifying protection tools; - organization of the protection structure, etc. The general principles of operation of the respective systems based on individual servers and software-emulated networks are considered. The main disadvantages of this technology are formulated. Attention is drawn to the prospects of using various Honeypot solutions to expand the potential of already deployed information security tools (IS).

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: Ноябрь 2019.

Авторы:

Сабина Рузудженк, студентка факультета компьютерных наук, ХНУ имени В.Н. Каразина, Харьков, Украина.
E-mail: ruzudzhenk.jb@gmail.com

Карина Погорелая, студентка факультета компьютерных наук, ХНУ имени В.Н. Каразина, Харьков, Украина.
E-mail: karina.pogorelka@gmail.com
Татьяна Кохановская, студентка факультета компьютерных наук, ХНУ имени В.Н. Каразина, Харьков, Украина.
E-mail: kate7smith12@gmail.com
Сергей Малахов, к.т.н., с.н.с., доц. кафедры, ХНУ имени В.Н. Каразина, Харьков, Украина.
E-mail: mailgate@meta.ua

Особенности защиты корпоративных ресурсов с помощью технологии Honeypot.

Аннотация. В статье представлен краткий обзор основных возможностей технологии Honeypot. Рассмотрены вопросы касающиеся: - особенностей мониторинга сетевой активности на разных этапах развития атаки/вторжения; - размещения датчиков системы; - процедур сбора и обобщения данных о сетевых событиях; - вариантов модификации инструментов защиты; - организации структуры защиты и т.п. Рассмотрены общие принципы работы соответствующих систем на базе отдельных серверов и программно эмулируемых сетей. Обобщены основные недостатки данной технологии. Обращено внимание на перспективность использования различных решений Honeypot для целей расширения потенциала уже развернутых средств обеспечения информационной безопасности (ИБ).

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