INFORMATION WARFARE

DOI 10.20535/2411-1031.2021.9.2.249897
УДК 004.056(53+57)

АРТЕМ ЖИЛІН,
ОЛЬГА ШЕВЧУК

АРХІТЕКТУРА ТА КЛАСИФІКАЦІЯ DECEPTION TECHNOLOGY

У зв'язку зі стрімким зростанням та модифікацією хакерських атак, актуальним питанням стає дослідження різних засобів захисту, які б дозволяли аналізувати поведінку зловмисника в мережі. Відомі методи захисту мають свої недоліки і в більшості випадків не дозволяють проаналізувати дії нападника в ході реалізації атаки. Для вирішення цих задач розробляються нові технології захисту, відомі як Deception Technology, які дозволять зменшити завантаженість системи (кількість подій безпеки) і допомагають аналізувати дії зловмисника в режимі реального часу. В статті досліджується Deception Technology як технологія яка не тільки долає основний недолік стандартних засобів захисту, а саме велику кількість згенерованих подій безпеки, які потрібно обробляти, зберігати та реагувати на них, а й дозволяє досліджувати й аналізувати дії зловмисників. Задля точного та правильного використання даної технології постає питання дослідження її розвитку та класифікації рішень. Тому основною задачею, яка вирішувалась, є класифікація Deception Technology. Разом з подоланням недоліків стандартних засобів захисту виникає завдання доведення результативності технології. Реалізацію Deception Technology проведено на прикладі рішення T-Pot, компонентами якої є достатньо велика кількість honeypot, що емулюють мережеві сервіси. Результатом роботи є запропонована класифікація Deception Technology та опис її архітектури. Як приклад, показано реалізацію проаналізованого класу захисту з метою доведення результативності його роботи в режимі реального часу і визначено, що у зв'язку з невеликою кількістю інформації, що збирається, досить легко зіставити й ідентифікувати той напрям безпеки системи, який не опрацьовано адміністраторами безпеки. При перегляді статистики використання логінів і паролів визначено найуживаніші, а саме числові паролі "1234" та "123456", які за останні роки є найбільш використовуваними зловмисниками при зломі систем.

Ключові слова: технологія обману, приманка, T-Pot, засоби захисту.

Постановка проблеми. В час активного розвитку комп'ютерних технологій і мереж хакерські атаки стають більш поширеними, різноманітними та багатокроковими, що призводить до погіршення працездатності системи, до втрати особистих даних і контролю над системою. Разом з відомими типами атак починають з'являтися нові, а раніше відомі атаки піддаються модифікації з боку зловмисників [1], [2].

Фахівці з захисту комп'ютерних мереж намагаються запобігти вторгненням за допомогою традиційних технологій захисту, таких як міжмережевий екран, технології виявлення і запобігання вторгненням, сканери вразливостей та мережеві аналізатори. Переваги та недоліки деяких з цих технологій наведені у [3], [4]. Однак, можливості таких периметричних засобів захисту є недостатніми, а варіативні вразливості об'єктів та систем захисту породжують множину атак, яку ці засоби захисту не в змозі попередити.

Незважаючи на те, що традиційні засоби захисту є важливими компонентами системи захисту, вони мають свої недоліки. Одним з основних недоліків традиційних засобів захисту, що використовуються, є велика кількість згенерованих подій безпеки, які потрібно зберігати, обробляти та реагувати на них. В той же час існують рішення класу Deception Technology, які дозволяють зменшити кількість подій безпеки і допомагають досліджувати дії зловмисника в режимі реального часу. Однак, на даний час відсутня повна класифікація цієї технології. Тому актуальною є задача дослідження рішення класу Deception Technology.

Аналіз останніх досліджень і публікацій. Рішення класу Deception Technology почало з'являтися зовсім нещодавно. Йому передував етап розвитку таких систем як honeypot. В [5] наведено основні концепції, підходи і проблеми honeypot. В [6] визначено переваги та недоліки різних honeypot. Водночас, [7], [8], [9], [10] підтверджують зростаючу популярність Deception Technology. У [11] встановлено переваги та основні принципи роботи Deception Technology, а також відмінності технології Deception Technology і honeypot. У [12] описано налаштування T-Pot, як рішення класу Deception Technology. Однак, в жодній з цих публікацій не надано класифікацію нової технології Deception Technology, статистичні дані роботи Deception Technology й не доведено її результативності у ході виявлення атак та аналізу дій зловмисника в реальному часі.

Метою даної роботи є формування можливих варіацій використання Deception Technology на основі потрібних вимог, а також доведення її результативність у ході виявлення атак та дій зловмисника.

Виклад основного матеріалу дослідження. У наш час існують підходи, які зменшують кількість згенерованих повідомлень про роботу системи та підвищують ефективність вже відомих систем захисту. Одним з цих підходів є honeypot.

Honeypot – це ресурс, що являє собою приманку для зловмисників, метою якої є дослідження атак та несанкціонованого доступу до систем. За допомогою цієї системи можна вивчити стратегію зловмисника та визначити перелік технік, тактик та процедур, за допомогою яких може бути завдана шкода і системам і реально існуючим об'єктам захисту [13].

Одержану honeypot інформацію можна умовно розділити на дві частини:

– зібрана інформація про зловмисника (IP адреса, утиліти, що використовуються при атаці, частота атак);

– інформація, що дозволяє адміністратору перевірити стан системи (як приклад, поточне використання процесора).

Методів отримання такої інформації є два [14]: прямо на хості з honeypot – host–based, і віддалене отримання – network–based (див. рис. 1).

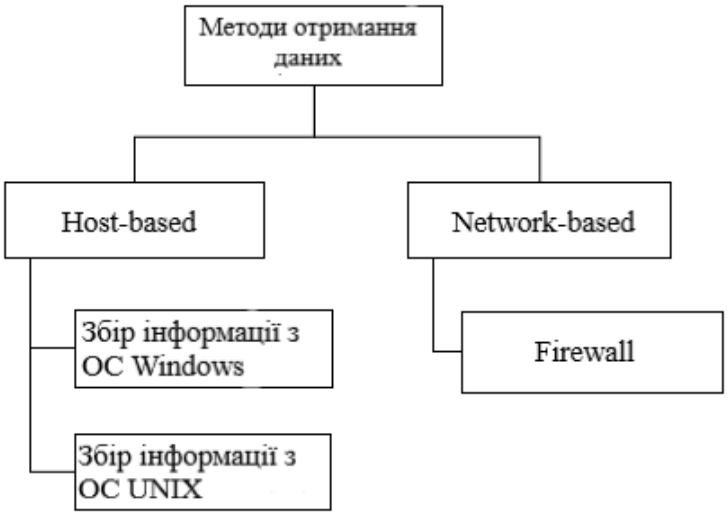

Рисунок 1 – Методи отримання даних honeypot

Разом з honeypot також існують інші схожі системи. Першою з яких є honeytoken. Honeytoken – це будь-який ресурс, який зберігається або обробляється комп'ютерною системою. Зазвичай honeytoken являє собою текстовий файл, повідомлення електронної пошти або запис бази даних до яких не звертаються в звичайних умовах під час автономної роботи. Інакше кажучи, будь-який доступ до даних honeytoken слід розглядати як шкідливий вплив [15].

Сукупність взаємопов'язаних honeypot, яка координує свої зусилля для забезпечення активного захисту мережі, називаються honeynet. Вона може бути відокремлена від робочої мережі. Керуючий трафік, що потрапляє в honeynet, повинен фіксуватися honeypot. При проектуванні honeynet (див. рис. 2) можна налаштувати honeypot з низьким рівнем взаємодії, який буде перенаправляти запити на певні порти на honeypot з високим рівнем взаємодії (або інший з низьким рівнем взаємодії). Таким чином, служби на визначених портах будуть добре емулюватися, в той час як на інших портах деякі мережеві пакети будуть як і раніше реєструватися [16].

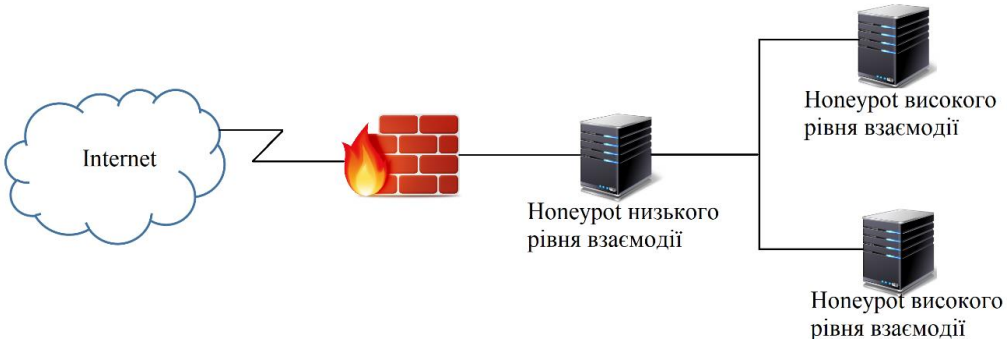

Рисунок 2 – Honeypot з низьким рівнем взаємодії, що перенаправляє обраний трафік на honeypot з високим рівнем взаємодії

Для успішної реалізації honeynet потрібно правильно розгорнути її архітектуру. Основою архітектури honeynet є honeywall – що призначена для аналізу трафіку, який транслюється з honeypot або ж на нього. Його можна використовувати для моніторингу і контролю всіх вхідних і вихідних з'єднань з honeynet. Honeywall дозволяє перехоплювати необроблений трафік в форматі PCAP (Packet Capture) й аналізувати мережеві потоки.

Honeywall складається з трьох основних частин – вебінтерфейс, модуль аналізу даних і модуль візуалізації, які працюють спільно [15]. Основна мета вебінтерфейсу honeywall – дозволити користувачеві вивчати події, що відбуваються в honeynet. Модуль аналізу даних здатний перехоплювати дані, що надходять з honeypot, і зіставляти їх з мережевим трафіком. На основі цієї інформації модуль візуалізації може представити деревовидний графік процесів, які вони викликали на атакованих машинах. Весь трафік, що проходить через honeywall, розбивається на окремі потоки і відображається у вигляді списку з інформацією про: час події, виявлену операційну систему зловмисника, IP адреси, які беруть участь в обміні даними, обсяг трафіку і кількість пакетів, обмін між кінцевими точками, і, нарешті, служба (номер порту і протокол), яка піддається атаці. Оператор може виконати подальший аналіз потоків, вивчивши результати спрацювання honeypot [15].

Подальше логічне об'єднання цих рішень призвело до появи нових засобів, таких як Deception Technology [17]. На рис. 3 показано систему компонентів Deception Technology й місце кожного проаналізованого вище компоненту.

Deception Technology відноситься до ряду досконаліших продуктів ніж honeypot і honeynet, які забезпечують більшу автоматизацію як для виявлення, так і для реалізації захисту на основі даних, які вони збирають. Важливо визначити, що існують різні рівні Deception Technology. Деякі з них є чимось більшим, ніж просто honeypot, а інші імітують повноцінні мережі, які містять реальні дані і пристрої. Це дозволяє виявляти атаки на її початку, збирати відомості про можливі загрози і виявляти зловмисника перш ніж він зможе завдати якої-небудь суттєвої шкоди.

Deception Technology працює інакше, ніж традиційні системи захисту комп'ютерних мереж. Традиційні засоби захисту мають тенденцію працювати безпосередньо з діями зловмисника, наприклад, щоб запобігти їм або виявити. Deception Technology дозволяє

маніпулювати мисленням зловмисника, змушуючи його діяти так, щоб це було вигідно захиснику. Будучи принципово іншою за будовою, Deception Technology може бути ефективнішою там, де традиційні засоби захисту мають недоліки. По-перше, дана технологія може відвернути увагу атакуючого від реальних цілей і ресурсів, збільшуючи його свободу дій. По-друге, може привести до того, що атакуючий буде діяти так, що це спрацює на користь захисника. По-третє, дана технологія може допомогти захиснику несподівано виявити зловмисника. Нарешті, Deception Technology може захистити реальні ресурси від руйнування. Мета Deception Technology – запобігти зловмиснику, який встиг проникнути в мережу, завдати будь-яких суттєвих втрат.

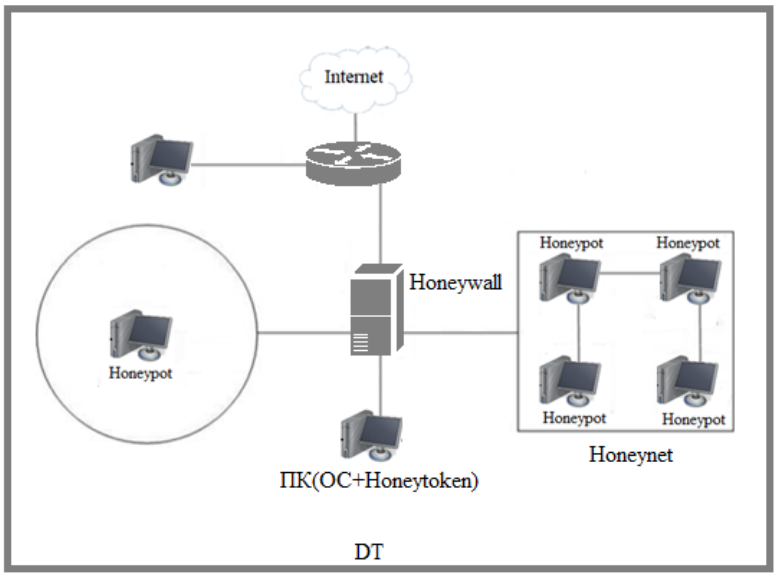

Рисунок 3 – Honeypot, honeynet, honeytoken та honeywall як складові Deception Technology

Deception Technology є сукупністю технік імітації інфраструктури інформаційних технологій та дезінформації зловмисників, які використовуються з метою:

– порушення засобів автоматизації зловмисника та затримки його дій або ж порушення процесу атаки;

– виявлення атаки та уповільнення її прогресу, що в результаті дозволяють зупиняти атаки до нанесення значного збитку;

– звернення уваги зловмисника на себе, щоб відвернути його від реальних ресурсів, при цьому зібрати інформацію про місцезнаходження зловмисника, інструменти і методи атак.

Крім попередньо розглянутих honeypot та honeywall до компонентів архітектури Deception Technology належать (див. рис. 4) [18]:

1. Модуль моніторингу – це модуль оцінки загроз, який відстежує мережеві і/або системні дії на предмет шкідливих дій або порушень політики і створює звіти. Перегляд порядку, послідовності, відміток часу і типу пакетів, які використовуються зловмисником для отримання доступу до honeypot, і натискання клавіш, доступ до системи, змінені файли, допомагають визначити інструменти та методологію, яка використовується зловмисниками, і їх наміри (вандалізм, крадіжка даних, пошук в точці віддаленого запуску). Роботу блоку моніторингу може виконувати система виявлення вторгнень.

2. Модуль сповіщення – повинен мати можливість генерувати повідомлення електронною поштою, щоб відправляти адміністратору повідомлення про трафік, що йде на honeypot чи з нього, щоб він міг переглядати дії зловмисника, поки вони відбуваються.

3. Блок реєстрації – цей блок забезпечує ефективне сховище для всіх журналів міжмережевого екрану і системи, а також трафіку, що проходить через міжмережевий екран і систему honeypot.

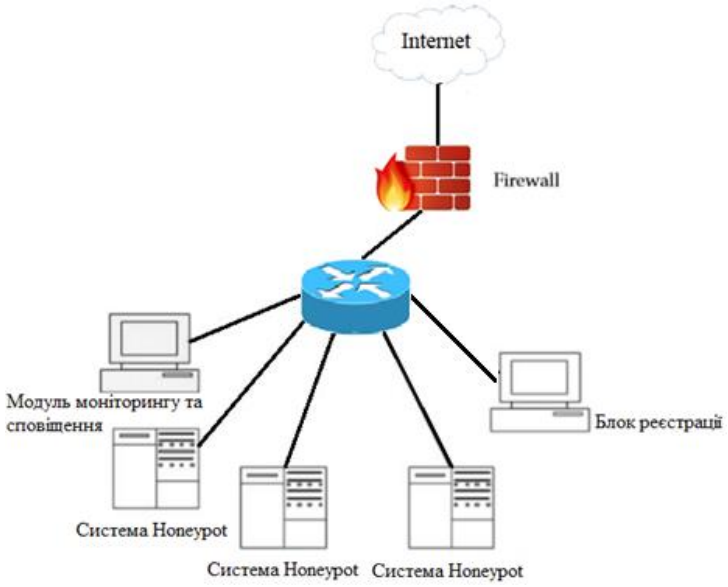

Рисунок 4 – Загальна архітектура Deception Technology

Стратегія даної технології полягає в безпечному відключенні зловмисників від виробничих систем, переключенні їх до Deception Technology та отриманні інформації про зловмисників шляхом реєстрації їх дій [18]. На рис. 5 показаний приклад того, як Deception Technology може бути розгорнута в мережі з метою захисту. У цьому прикладі Honeypot - A моделює систему без будь-якого firewall або системи виявлення вторгнень (IDS); Honeypot - B імітує вразливу службу типу Ftp або Telnet, щоб привернути увагу зловмисника; Honeypot - C і Honeypot - D імітують інші системи в мережі організації, щоб відвернути зловмисника від реальних систем.

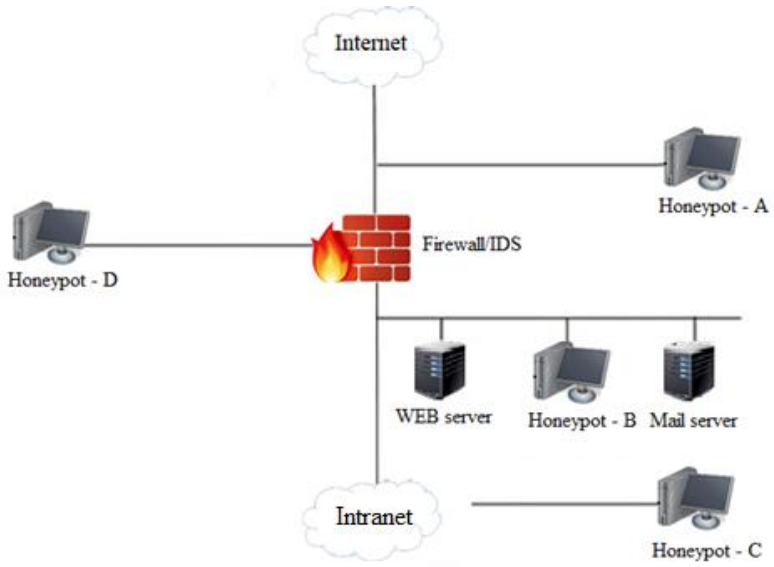

Рисунок 5 –Приклад розгортання Deception Technology в мережі

Актуальною є класифікація Deception Technology за різними ознаками, для їх правильного використання у системах захисту. Так, як Deception Technology – це об`єднання декількох засобів захисту (honeypot, honeywall), то при класифікації за визначеними категоріями дану технологію можна об’єднати з цими засобами захисту.

На рис. 6 представлено класифікацію існуючих типів Deception Technology за чотирма основними та незалежними критеріями (класами): за видом, за типом атакованих ресурсів, за рівнем взаємодії та за спеціалізацією.

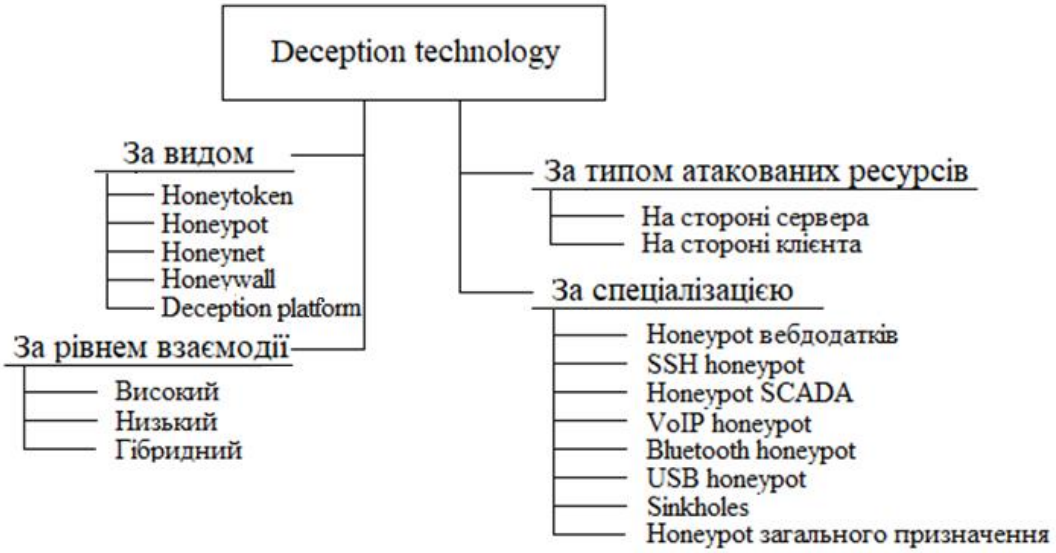

Рисунок 6 – Класифікація існуючих типів Deception Technology

Перший критерій (клас) – за типом атакованих ресурсів описує, чи використовуються ресурси honeypot у режимі сервера чи клієнта. Honeypot на стороні сервера діють як сервери, тобто надають відкритий порт, кілька портів та пасивно прослуховують вхідні з'єднання, встановлені віддаленими (ймовірно, шкідливими) клієнтами. Часто такі типи honeypot виявляють загрози, які використовують сканування як засіб виявлення потенційних жертв для компрометації. Honeypots на стороні клієнта, призначені для виявлення атак на клієнтські програми. Клієнтські honeypot достатньо відрізняються своєю роботою від серверних. Вони активно встановлюють з'єднання з сервісами, щоб виявити шкідливу поведінку серверу або контенту.

Другий критерій (клас) – за рівнем взаємодії визначає, чи є honeypot реальним ресурсом (з високим рівнем взаємодії) або тільки емуляцією (низький рівень взаємодії). Змішаний тип honeypot, який поєднує обидві функції, називається гібридним. Різниця між ними полягає в тому, що приманки з низькою взаємодією легше розгортати і обслуговувати, а сама емуляція знижує ризик злому системи. Приманки з високим рівнем взаємодії визначають реальну поведінку операційної системи під час атаки та здатні виявляти атаки на вразливості нульового дня.

Третій критерій (клас) – за спеціалізацією. Цей критерій визначає, яка служба або метод атаки/виявлення є основною областю дії honeypot.

Існує велика варіація можливих значень цього класу. Нижче представлені одні з найпопулярніших:

1. Honeypot вебзастосунків – інструменти, призначені для виявлення атак на вебдодатки;
2. SSH honeypot – інструменти, орієнтовані на атаки Secure Shell (SSH);
3. Honeypot SCADA – інструменти, адаптовані під промислові системи управління;
4. VoIP honeypot – інструменти виявлення загроз в Інтернет-телефонії (Voice over IP);
5. Bluetooth honeypot – інструменти, призначені для виявлення атак, що поширюються за технологією Bluetooth;
6. USB honeypot – інструменти, призначені для виявлення атак за допомогою USB-пристроїв;
7. Sinkholes – інструменти, що використовують "техніку провалів" для виявлення та моніторингу інфекцій в мережі;
8. Honeypot загального призначення – інструменти, призначені для виявлення більш ніж однієї техніки атаки або декількох служб.

Четвертий критерій (клас) було описано при визначенні поняття honeypot.

З метою обґрунтування результативності Deception Technology при виявленні атак та дій зловмисника було обрано T-Pot. Проєкт T-Pot – це програмне забезпечення з відкритим вихідним кодом – монітор інцидентів на основі приманок, який розроблено і використовується Deutsche Telekom. Програмний продукт T-Pot є платформою приманки з посиленим виявленням і реагуванням, з можливістю ретельного моніторингу і вивчення зловмисників. T-Pot надає багаточислені демони honeypot, які працюють паралельно, і перенаправляє трафік, захоплений мережевим інтерфейсом, на доступний honeypot з відкритим кодом. Дані оброблюються і зберігаються в локальному стеку ELK (англ. Elastic Stack) . Архітектура та принципи роботи T-Pot описані у [19], [20].

T-Pot підтримує такі honeypot – adbhoney, ciscoasa, conpot, cowrie, dionaea, elasticpot, glutton, heralding, honeypy, honeytrap, mailoney, medpot, rdpy, snare/tanner, розміщені в контейнерах. Кожний з вкладених honeypot відповідає різним завданням. Детально кожен honeypot проаналізовано у [21]. В даній статі описані лише ті honeypot, які використовувались в ході реалізації.

Ciscoasa – honeypot з низьким рівнем взаємодії, здатний виявляти CVE-2018-0101, вразливість DoS та віддалене виконання коду на 5000udp та 8443 портах.

Cowrie – це SSH і Telnet honeypot з низьким і високим рівнем взаємодії, призначені для реєстрації атак з використанням “грубої сили”. В режимі низького рівня взаємодії він емулює систему UNIX, в режимі високого рівня взаємодії (проксі) він функціонує як SSH і проксі telnet для спостереження за поведінкою зловмисника в іншій системі. Задіяні 22 та 23 порти.

Honeytrap – це інструмент мережевої безпеки, призначений для спостереження за атаками на TCP і UDP. Він працює як демон і запускає сервісні процеси динамічно на запитувані порти. Сервер емулює відому службу, надсилаючи захоплений мережевий трафік на підключений хост.

Система T-Pot використовує переваги контейнерів, для забезпечення високого ступеня розгортання системи. Контейнерні honeypot, які підтримуються платформою T-Pot, активно допрацьовуються розробниками й призначені для різних рівнів інтерактивності та атакуючих.

Задля спрощення аналізу даних використовується стек (ELK), який дозволяє класифікувати та візуалізувати дані складних атак. Крім того, всі дані, отримані демонами honeypot, відображаються на зручних панелях інструментів, які дозволяють користувачам переглядати зібрані дані, аналізувати атаки і досліджувати ці дані.

Кожен honeypot визначається як dockerfile, який вбудований в образ. Потім цей образ використовується для запуску honeypot, і дані, що ним генеруються, зберігаються в томах, які спільно використовуються з хост-системою.

Для підтвердження отриманих результатів поставлено експеримент з метою доведення результативності Deception Technology та виявлення атак в сегменті мережі, в якій використовувались такі honeypot як Cowrie і Conpot, що відповідають за 22, 23 та 80 порт.

Протягом 30 днів за допомогою Deception Technology було зареєстровано 1647547 атак.

Проаналізувавши дані, було визначено:

- honeypot, які зазнали атаки: Cowrie, Tanner, Ciscoasa та Honeytrap;
- найбільш атакованими портами були 80 (HTTP) та 22 (SSH);
- були здійснені атаки типу підбір логіну/паролю, сканування портів;
- топ-3 країн зловмисників: Ірландія, Китай, Росія;
- топ-5 логінів, які використовувались при підборі, та числовий показник їх застосування:
    1. root – 105,652;
    2. admin – 46,318;
    3. guest – 24,441;
    4. user – 21,467;
    5. nproc –2,020.

– топ-5 паролів, які використовувались при підборі, та числовий показник їх застосування:

1. root – 59,787;
2. guest –24,096;
3. user – 19,924;
4. 123456 – 13,657;
5. 1234 – 3,595.

Під час аналізу результатів роботи T-Pot виявлено, що більшість паролів, які використовувалися зловмисниками, входять до актуального словника паролів що використовуються зловмисниками для взлому систем [21].

– операційні системи зловмисників, які були задіяні в атаках – Linux та Windows;
– вразливості інформаційної безпеки за CVE та числовий показник їх використання:
  1. CVE-2019-12263, CVE-2019-12261, CVE-2019-12260, CVE-2019-12255 – 56.
  2. CVE-2006-3602, CVE-2006-4458, CVE-2006-4542 – 2.
  3. CVE-2002-0013, CVE-2002-0012 – 1.

Висновки. Deception Technology є новою технологією захисту. Засоби honeypot, які є її основою, в порівнянні з іншими системами збирають невелику кількість даних, але ці дані мають велике значення. Honeypot може дати точну інформацію у швидкому та легкому для розуміння форматі. Це спрощує аналіз і зменшує час реакції на можливі атаки. Ці дані можуть бути використані для статистичного моделювання, аналізу дій, виявлення нападів або дослідження дій зловмисників. Крім того, у зв'язку з невеликою кількістю інформації, що збирається, досить легко зіставити й ідентифікувати той напрямок безпеки, який не було опрацьовано адміністраторами безпеки.

Представлена класифікація показує, що Deception Technology можна представляти за різними критеріями (за видом, типом атакованих ресурсів, рівнем взаємодії та за спеціалізацією), що дає можливість виокремлювати різні варіант побудови Deception Technology.

Для дослідження Deception Technology розгорнуто T-Pot, в ході безперервної роботи якої, отримано низку даних. У результаті їх аналізу визначено, що найбільш вразливими виявились honeypot, які відповідають за 80 і 22 порти (http і dns служби). Типами атак, які проводили зловмисники за період роботи T-Pot, були підбір паролю та сканування портів. При перегляді статистики використання логінів і паролів визначено найуживаніші. Особливу увагу слід звернути на числові паролі, а саме "1234" та "123456", які за останні роки є найбільш використовуваними зловмисниками при зломі систем жертв.

Отже, Deception Technology багатокомпонентне розгалужене рішення захисту, яке в режимі реального часу дозволяє слідкувати за діями зловмисника при виконанні атаки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Актуальные киберугрозы: IV квартал 2021 года, 2021. [Электронный ресурс]. Доступно: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q4/. Дата обращения: Авг. 11, 2021.

[2] Актуальные киберугрозы: итоги 2020 года, 2021. [Электронный ресурс]. Доступно: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/. Дата обращения: Авг. 11, 2021.

[3] Системы обнаружения и предотвращения вторжений, 2015. [Электронный ресурс]. Доступно: https://wiki.merionet.ru/seti/2/ids-ips/. Дата обращения: Авг. 15, 2021.

[4] Достоинства и недостатки основных технологий межсетевых экранов, 2015. [Электронный ресурс]. Доступно: https://studfile.net/preview/4431318/page:9/. Дата обращения: Авг. 15, 2021.

[5] I. Mokube, and M. Adams, "Honeypots: Concepts, Approaches, and Challenges", in *Proc. of the 45th Annual Southeast Regional Conference*, New York, pp. 321-326, 2007, doi: https://doi.org/10.1145/1233341.1233399.

[6] C. Keong NG, L. Pan, and Y. Xiang, *Honeypot Frameworks and Their Applications: A New Framework*, Singapore: Springer, 2018, doi: https://doi.org/10.1007/978-981-10-7739-5.
[7] Технология обмана, 2020. [Электронный ресурс]. Доступно: https://xakep.ru/2020/07/28/deception. Дата обращения: Авг. 27, 2021.
[8] What is Deception Technology, 2017. [Online]. Available: https://www.forcepoint.com/cyber-edu/deception-technology. Accessed on: Aug. 20, 2021.
[9] Deception technology, 2016. [Online]. Available: https://www.csoonline.com/article/3113055/deception-technology-grows-and-evolves.html. Accessed on: Aug. 27, 2021.
[10] S. A. Faulkner, "Looking to Deception Technology to Combat Advanced Persistent Threats", a dissertation project, Utica College, 2017.
[11] Deception technology, 2020. [Электронный ресурс]. Доступно: https://habr.com/ru/company/tssolution/blog/522374/. Дата обращения: Авг. 30, 2021.
[12] T-POT, 2016. [Online] Available: http://epistasislab.github.io/tpot/using/. Accessed on: Sept. 10, 2021.
[13] Приманка, 2018 [Электронный ресурс]. Доступно: https://www.techtarget.com/searchsecurity/definition/honey-pot. Дата обращения: Авг. 30, 2021.
[14] Развертывание IDS, 2013 [Электронный ресурс]. Доступно: https://intuit.ru/studies/courses/20/20/lecture/633?page=3#keyword89. Дата обращения: Авг. 30, 2021.
[15] P. Lackner, "How to Mock a Bear: Honeypot, Honeynet, Honeywall & Honeytoken: A Survey". [Online]. Available: https://www.insticc.org/node/TechnicalProgram/iceis/2021/presentationDetails/104000. Accessed on: Aug. 30, 2021.
[16] Технологии Honeypot. Часть 2: Классификация Honeypot, 2006. [Электронный ресурс]. Доступно: https://www.securitylab.ru/analytics/275775.php. Дата обращения: Сент. 12, 2021.
[17] Deception technology, 2019. [Online]. Available: https://www.gartner.com/en/documents/3939890/solution-comparison-for-six-threat-deception-platforms. Accessed on: Sept. 17, 2021.
[18] R. C. Joshi, and A. Sardana, *Honeypots A New Paradigm to Information Security*. Boca Raton: CRC Press, 2011.
[19] T-POT, 2018. [Online]. Available: https://cyber-99.co.uk/t-pot-honeypot-framework-installation. Accessed on: Sept. 25, 2021.
[20] T-POT, 2020 [Online]. Available: https://github.com/telekom-security/tpotce. Acceessed on: Sept. 10, 2021.
[21] Пароли [Электронный ресурс]. Доступно: https://www.tadviser.ru/index.php. Дата обращения: Сент. 10, 2021.

Стаття надійшла до редакції 30.09.2021.

REFERENCE

[1] Topical cyber threats: IV quarter of 2021, 2021. [Online]. Available: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q4/. Accessed on: Aug. 11, 2021.
[2] Current cyber threats: results of 2020, 2021. [Online]. Available: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/. Accessed on: Aug. 11, 2021.
[3] Intrusion detection and prevention systems, 2015. [Online]. Available: https://wiki.merionet.ru/seti/2/ids-ips/. Accessed on: Aug. 15, 2021.
[4] Advantages and Disadvantages of Firewall Technologies, 2015. [Online]. Available: https://studfile.net/preview/4431318/page:9/. Accessed on: Aug. 15, 2021.
[5] I. Mokube, and M. Adams, "Honeypots: Concepts, Approaches, and Challenges", in *Proc. of the 45th Annual Southeast Regional Conference*, New York, pp. 321-326, 2007, doi: https://doi.org/10.1145/1233341.1233399.
[6] C. Keong NG, L. Pan, and Y. Xiang, *Honeypot Frameworks and Their Applications: A New Framework*, Singapore: Springer, 2018, doi: https://doi.org/10.1007/978-981-10-7739-5.
[7] Deception technology, 2020. [Online]. Available: https://xakep.ru/2020/07/28/deception. Accessed on: Aug. 27, 2021.

[8] What is Deception Technology, 2017. [Online]. Available: https://www.forcepoint.com/cyber-edu/deception-technology. Accessed on: Aug. 20, 2021.
[9] Deception technology, 2016. [Online]. Available: https://www.csoonline.com/article/3113055/deception-technology-grows-and-evolves.html. Accessed on: Aug. 27, 2021.
[10] S. A. Faulkner, "Looking to Deception Technology to Combat Advanced Persistent Threats", a dissertation project, Utica College, 2017.
[11] Deception technology, 2020. [Online]. Available: https://habr.com/ru/ company/tssolution/blog/522374/. Accessed on: Aug. 30, 2021.
[12] T-POT, 2016. [Online] Available: http://epistasislab.github.io/tpot/using/. Accessed on: Sept. 10, 2021.
[13] Honeypot, 2018 [Online]. Available: https://www.techtarget.com/searchsecurity/definition/honey-pot. Accessed on: Aug. 30, 2021.
[14] IDS Deployment, 2013. [Online]. Available: https://intuit.ru/studies/courses/20/20/lecture/633?page=3#keyword89. Accessed on: Aug. 30, 2021.
[15] P. Lackner, "How to Mock a Bear: Honeypot, Honeynet, Honeywall & Honeytoken: A Survey". [Online]. Available: https://www.insticc.org/node/TechnicalProgram/iceis/2021/presentationDetails/104000. Accessed on: Aug. 30, 2021.
[16] Honeypot Technologies. Part 2: Honeypot Classification, 2006. [Online]. Available: https://www.securitylab.ru/analytics/275775.php. Accessed on: Sept. 12, 2021.
[17] Deception technology, 2019. [Online]. Available: https://www.gartner.com/en/documents/3939890/solution-comparison-for-six-threat-deception-platforms. Accessed on: Sept. 17, 2021.
[18] R. C. Joshi, and A. Sardana, *Honeypots A New Paradigm to Information Security*. Boca Raton: CRC Press, 2011.
[19] T-POT, 2018. [Online]. Available: https://cyber-99.co.uk/t-pot-honeypot-framework-installation. Accessed on: Sept. 25, 2021.
[20] T-POT, 2020 [Online]. Available: https://github.com/telekom-security/tpotce Acceessed on: Sept. 10, 2021.
[21] Passwords. [Online]. Available: https://www.tadviser.ru/index.php. Acceessed on: Sept. 10, 2021.

ARTEM ZHYLIN,
OLHA SHEVCHUK

DECEPTION TECHNOLOGY: ARCHITECTURE AND CLASSIFICATION

Due to the rapid growth and modification of hacker attacks, it is important to study security measures that would allow analyzing the behavior of an attacker on the network. Known methods of defense have their drawbacks and in most cases do not allow analyzing the actions of the attacker during the deployment of the attack. To solve these problems, new protection technologies are beginning to emerge, known as Deception Technology, which can reduce the load on the system (the number of security events) and help investigate the actions of an attacker in real time. The article discusses Deception Technology as a technology that not only eliminates the main drawback of standard security tools, namely the large number of generated security events that need to be processed, stored and responded to, but also allows you to investigate and analyze the actions of attackers. For the accurate and correct use of this technology, the question arises of studying its development and classifying solutions. Therefore, the main task that was being solved was the classification of Deception Technology. Along with overcoming the shortcomings of standard means of protection, the task of proving the effectiveness of the technology arises. The implementation of Deception Technology is carried out on the example of the T-Pot solution, the components of which are a fairly large number of honeypots that emulate network services. As a result of the work, a classification of Deception Technology and a description of its architecture are proposed. As an

example, the implementation of the analyzed protection class is shown in order to prove the effectiveness of its work in real time and it is determined that due to the small amount of information collected it is easy to compare and identify the security area of the system. When viewing statistics on the use of logins and passwords, the most frequently used ones were identified, namely, the numeric passwords “1234” and “123456”, which in recent years have been the most used by cybercriminals in hacking systems.

Keywords: Deception Technology, honeypot, T-Pot, protection systems.

Жилін Артем Вікторович, кандидат технічних наук, доцент, професор кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID ID 0000-0002-4959-612X, zhylinartem@gmail.com.

Шевчук Ольга Сергіївна, викладач-стажист кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна, ORCID ID 0000-0002-2866-439X, olia13511@gmail.com.

Zhylin Artem, candidate of technical sciences, associate professor, professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.

Shevchuk Olha, trainee teacher at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine “Igor Sikorsky Kyiv polytechnic institute”, Kyiv, Ukraine.