УДК 004.56

**Д. В. Наумчак**
**Л. М. Куперштейн**

# ОСОБЛИВОСТІ ЗАСОБІВ HONEYPOT У КОНТЕКСТІ ВЗАЄМОДІЇ ЗІ ЗЛОВМИСНИКОМ

Вінницький національний технічний університет

**Анотація**
*Проаналізовано класифікацію засобів Honeypot за ступенем взаємодії зі зловмисником. Розглянуто їх призначення та функціональні характеристики.*
**Ключові слова:** кібербезпека, вразливість, приманка.
**Abstract**
*The classification of Honeypot tools according to the degree of interaction with the attacker is analyzed. Their purpose and functional performances are considered.*
**Keywords:** cybersecurity, vulnerability, honeypot.

## Вступ

Honeypot – обладнання або ПЗ, які спеціально розгортаються відділами безпеки для вивчення загроз [1]. Honeypot служить приманкою для зловмисників, щоб спонукати їх вторгнутися в мережу для будь-якого незаконного використання. Такі приманки зазвичай налаштовуються для вивчення активності зловмисника в мережі, щоб розробити більш надійні засоби захисту. Honeypot не містять ніяких цінних даних, так як це підроблений хост, який допомагає реєструвати мережевий трафік.

Виходячи цього, Honeypot зазвичай збирає такі дані [2]:

- IP-адреса зловмисника;
- Поєднання клавіш які вводяться зловмисником;
- Дані до яких зловмисник отримав доступ, видалив чи змінив;
- Імена користувачів і різні привілеї, які використовуються зловмисником.

## Результати дослідження

В даний час існує класифікація засобів Honeypot за ступенем взаємодії зі зловмисником [3-5]:

- слабка взаємодія;
- середня взаємодія;
- сильна взаємодія.

Кожен з цих видів Honeypot надає певну функціональність, або рівень взаємодії зловмисника з системою. Таким чином, починаючи від Honeypot слабкої взаємодії, функціональні можливості Honeypot розширюються.

Засоби Honeypot слабкої взаємодії зазвичай досить просто встановити, налаштувати, використовувати і підтримувати, тому що вони мають просту структуру і базові функції [3, 4]. Як правило, дані Honeypot імітують тільки частина сервісів. Зловмисник обмежений у взаємодії з цими сервісами. Наприклад, Honeypot слабкої взаємодії може імітувати стандартний сервер Unix з декількома запущеними сервісами, такими як telnet або ftp. Зловмисник може створити з'єднання telnet до системи, отримати банер операційної системи і запит login. Після чого, зловмисник може здійснювати спроби підбору пароля, які будуть записуватися Honeypot, але справжньою операційної системи немає, і взаємодія зловмисника з системою на даному етапі закінчується.

Головна мета Honeypot слабкої взаємодії – виявлення, особливо, сканувань і несанкціонованих спроб з'єднання. В силу того, що дані Honeypot надають обмежену функціональність, більшість з них представляються у вигляді програм. Програма може бути просто встановлена на хост і налаштована відповідно до вимог. Завдання адміністратора в даному випадку - проводити моніторинг попереджень, які генерує Honeypot, а також відстежувати зміни імітованого програмного забезпечення.

Honeypot слабкої взаємодії рекомендується для індивідуального використання або для невеликих організацій. Також вони можуть бути використані для поліпшення розуміння даної технології.

Засіб Honeypot середнього взаємодії надає зловмисникові більше можливостей, ніж Honeypot слабкої взаємодії, але має меншу функціональність у порівнянні з Honeypot сильної взаємодії. Дані засоби можуть очікувати різну активність, і спроектовані давати кілька можливих відповідей на дії зловмисника.

Прикладом Honeypot середнього взаємодії є деякі можливості операційної системи Unix, такі як "chroot", або ж в Windows - Virtual Machine Ware (VMWare). Вони дозволяють адміністратору розбивати оточення операційної системи, створюючи віртуальні операційні системи всередині реальної. Віртуальне операційне система може контролюватися реальної операційною системою, але використання такої системи зовні дуже схоже зі справжньою. Сенс полягає в тому, що зловмисник буде взаємодіяти з підробленим оточенням, таким чином, вся його активність може бути контрольована з боку реальної операційної системи.

Однак даний підхід має кілька проблем. По-перше, дане рішення досить складне, таким чином, на стадії роботи або конфігурації можуть виявитися помилки. По-друге, надати віртуальному оточенню повну функціональність і взаємодія з реальною операційною системою - трудомістке завдання. Чим більше функціональності і реалістичності надається віртуальному оточенню, тим легше для зловмисника обійти дане оточення і отримати контроль над реальною операційною системою. Таким чином, більшість Honeypot середнього взаємодії не пропонують виконання усіх функцій стандартної операційної системи.

Honeypot середнього взаємодії вимагає кілька великих зусиль при установці і налаштуванні, ніж слабкої взаємодії. Зазвичай дані рішення не надаються у вигляді готових програмних рішень [5]. Для того, щоб ввести в експлуатацію подібний вид Honeypot потрібно детальне налаштування функціональності в порівнянні з Honeypot слабкої взаємодії.

Засоби Honeypot сильного взаємодії досить небезпечні. Вони надають більшу кількість інформації про зловмисників, але вимагають достатній час для побудови і підтримки. Крім того, приносять найвищий рівень ризику. Мета Honeypot сильної взаємодії – надати зловмисникові доступ до реальної операційній системі, де нічого не імітується або обмежується [3, 4]. Зручності для вивчення в даному випадку неймовірні. Існує можливість досліджувати нові засоби, виявляти нові вразливості в операційних системах або додатках, а також дізнаватися, яким чином зловмисники зв'язуються між собою.

Для створення подібного оточення, в принципі, не потрібно вносити будь-які зміни в реальні операційні системи. Більшість стандартних збірок не мають ніяких відмінностей щодо існуючих виробничих систем в більшості організацій. Єдина річ, яка визначає ці системи як Honeypot, – це те, що вони не мають виробничого значення. Їх мета – бути дослідженими, атакованими або скомпрометовані. Слід зробити висновок, що такий потужний засіб приносить величезний рівень ризику. Після отримання зловмисником повного доступу, він починає взаємодіяти з повнофункціональною операційною системою, яка надає йому можливість здійснювати будь-які дії, наприклад, атакувати інші системи або збирати внутрішній трафік. Великий обсяг роботи повинен полягати в зниженні цих ризиків.

У більшості випадків Honeypot сильної взаємодії розташовуються в контрольованому середовищі, наприклад, в мережі – після міжмережевого екрану. Здатність контролювати зловмисника відбувається не від самого Honeypot, а від контролюючого мережевого пристрою. Міжмережевий екран надає зловмисникові можливість атакувати засіб Honeypot, але забороняє виконувати зовнішні атаки. Так як побудована архітектура досить складна, то потрібно детально визначити базу правил брандмауера.

У табл 1. представлено зіставлення класифікацій за ступенем взаємодії і за значеннями ознак.

Таблиця 1

| Honeypot взаємодія | Процес встановлення та налаштування | Процес використання та підтримки | Збір даних | Рівень протоколювання | Рівень імітації | Рівень ризику |
|---|---|---|---|---|---|---|
| слабка | простий | простий | обмежений | низький | низький | низький |
| середня | середній | середній | змінний | середній | середній | середній |
| сильна | складний | складний | розширений | високий | високий | високий |

## Висновки

Honeypot служить для збору інформації про зловмисника, аналізу методів атак та захисту реального цільового ресурсу, яка використовується в багатьох ситуаціях. Не має значення, чим є ресурс: імітованим сервісом або повноцінною операційною системою. Головне, що сенс функціонування ресурсу полягає в нападі на нього. Як засоби здійснення безпеки, Honeypot мають ряд переваг. Вони мають здатність ефективно працювати в мережі, збираючи невелику кількість даних, при цьому велика частина цієї інформації має високе значення. Honeypot ефективно працюють в інтенсивному середовищі і вимагають невеликих затрат на розгортання. Але Honeypot мають низку недоліків. Найгірший з них полягає в тому, що звужується область бачення проблем. Якщо Honeypot не атакувати, то він не має нікого значення. Крім того, деякі Honeypot піддаються методам розкриття зловмисником і можуть бути виявлені або, гірше того, використані для проникнення в інші системи. Honeypot слабкої взаємодії рекомендується використовувати для невеликих компаній та для поліпшення розуміння даної технології. Для багатьох Honeyroy із середньою взаємодією є найкращим балансом, що забезпечує менший ризик, ніж створення повної фізичної або віртуалізованої системи для обману зловмисників, але з більшою функціональністю. Вони не підходять для складних загроз, таких як експлойти з нульовим днем, але можуть націлювати зловмисників, які шукають конкретні вразливості. Honeypot сильної взаємодії слід використовувати, коли адміністратор хоче надати повні права зловмиснику до системи, щоб потім проаналізувати його дії та дізнатись більше інформації про атаку та зловмисника.

## СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ


1. What is a honeypot? How it can lure cyberattackers. URL: https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html (дата звернення: 03.03.2021)
2. Addison Wesley, Lance Spitzner. Honeypots: Tracking Hackers: монографія. Boston: Wesley Longman Publishing Co., 2002. 41 p.
3. Iyad Kuwatly, Malek Sraj, Zaid AI Masri, and Hassan Artail. A Dynamic Honeypot Design for Intrusion Detection. *American University of Beirut.* 2004. URL: https://static.aminer.org/pdf/PDF/000/350/708/a_dynamic_honeypot_design_for_intrusion_detection.pdf( дата звернення: 04.03.2021)
4. Mr. Kartik Chawda ,Mr. Ankit D. Patel. Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring. *IEEE.* 2014 URL: http://www.cse.umich.edu/techreports/cse/2004/CSE-TR-499-04.pdf (дата звернення: 05.03.2021)
5. Iyatiti Mokube , Michele Adams. Honeypots. Concepts, Approaches, and Challenges. *Armstrong Atlantic State University.* 2007. URL: http://www.cs.potsdam.edu/faculty/laddbc/Teaching/Ethics/StudentPapers/2007Mokube-Honeypots.pdf (дата звернення: 05.03.2021)



***Наумчак Дмитро Валерійович*** – студент групи 2БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: naumchakdmytro@gmail.com.

***Купершейн Леонід Михайлович –*** к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

***Naumchak Dmytro V. –*** Student of Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, e-mail: naumchakdmytro@gmail.com.

***Kupershtein Leonid M.*** — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com