УДК 004.056.57

Технологія Honeypot для захисту комп'ютерної мережі

Войтович В.С., курсант,
Мандрона М.М., доцент
Львівський державний університет безпеки життєдіяльності, м. Львів

Honeypot – це комп'ютерна система, яка створена для того, щоб заманити кіберзлочинців, а також виявляти, відхиляти або вивчати спроби отримати несанкціонований доступ до інформаційних систем. Як правило, вона складається з комп'ютера, програм та даних, які імітують поведінку реальної системи, яка, як видається, є частиною мережі, але насправді є ізольованою і ретельно контролюється. Всі зв'язки з honeypot вважаються ворожими, оскільки немає підстав для законних користувачів доступу до honeypot. Перегляд та реєстрації даної діяльності дає змогу зрозуміти рівень та типи загрози мережевої інфраструктури, відволікаючи злочинців від активів реальної вартості [1].

На основі їх дизайну та розгортання, honeypots класифікуються як науково-виробничі honeypots. Дослідження honeypots запускаються для точного аналізу активності хакерів і того, як атаки розвиваються та розвиваються, щоб навчитися краще захищати системи від них. Дані, розміщені в honeypot з унікальними ідентифікаційними властивостями, також можуть допомогти аналітикам відслідковувати вкрадені дані та визначати зв'язки між різними учасниками атаки.

Виробничі honeypots розміщуються всередині виробничої мережі з іншими виробничими серверами у ролі приманки в рамках системи виявлення вторгнення в мережу (IDS) [2]. Їхнє призначення є для того, щоб вони відображалися справжніми та містили інформацію або ресурс, за допомогою якого можна залучити хакерів та зайняти їх. Це пов'язує час і ресурси зловмисника, надаючи адміністраторам час для оцінки та пом'якшення будь-яких уразливостей у своїх фактичних системах виробництва. Інформація, зібрана з honeypot також може бути корисною для виявлення та переслідування тих, хто стоїть за атакою. Дослідники підозрюють, що деякі кіберзлочинні особи також використовують honeypots для збору, розвідки про дослідників, виступають в якості дезінформаторів.

Honeypots з високим рівнем взаємодії імітують діяльність виробничої системи та отримують велику інформацію – чисті honeypots є повноцінними виробничими системами, використовуючи екран на посилання honeypot на мережу. Мета honeypots з високою взаємодією, полягає в тому, щоб зловмисник отримував кореневий доступ на машині, а потім вивчав те, що він робить. Зловмисник з кореневим доступом має доступ до всіх команд і файлів у системі, тому цей тип honeypot несе

найбільший ризик, але також має найбільший потенціал для збору інформації. Низькі взаємодії honeypots імітують тільки послуги, які часто націлені зловмисниками, і тому вони менш ризиковані та менш складні для підтримки. Віртуальні машини часто використовуються для розміщення honeypots, щоб honeypot можна було відновити швидше, якщо це скомпрометовано. Два або більше honeypot в мережі утворюють honeynet, а honeypty являє собою централізовану колекцію honeypots та інструменти аналізу.

Honeypots допомагають усвідомлювати загрози мережевим системам, але виробничі honeypots не повинні розглядатися як заміна стандартного IDS. Якщо вони не належним чином налаштовані, вони можуть бути використані для доступу до реальної виробничої системи або використовуватись як стартовий майданчик для атак проти інших систем [3].

Висновок: на сьогоднішній день найбільший інтерес представляють високоінтерактивні динамічні honeypot-системи, так як з завданнями низкоінтерактивних систем справляються інші елементи корпоративної мережі: мережеві сканування успішно запобігають міжмережевими екранами і системами виявлення та запобігання вторгнень, а також правильної конфігурацією елементів мережі, а інформація про конкретні дії зловмисника, вжитих для здійснення доступу в корпоративну мережу, надають набагато більшу цінність, ніж інформація про факт проникнення в мережу, яка також може бути отримана від міжмережевих екранів і засобів виявлення вторгнень.

Динамічні ж honeypot-системи мають великий потенціал розвитку. У таких системах можуть бути застосовані ідеї, зарекомендувавши себе в інших типах систем, а також запропоновані і принципово нові підходи.

Список літератури

1. Intrusion Detection FAQ: What is a Honeypot? [Електронний ресурс]. Режим доступу: https://www.sans.org/security-resources/idfaq/honeypot3.php
2. Dynamic Honeypots [Електронний ресурс]. Режим доступу: http://www.symantec.com/connect/articles/dynamic-honeypots
3. Гіпервізор, віртуалізація і хмара: Про Гіпервізор, віртуалізації систем і про те, як це працює в хмарному середовищі [Електронний ресурс]. Режим доступу: http://www.ibm.com/developerworks/ru/library/cl-hypervisorcompare/
4. The Honeynet Project [Електронний ресурс]. Режим доступу: https://www.honeynet.org