УДК 004.056.57

КЛАСИФІКАЦІЯ HONEYPOT ТЕХНОЛОГІЙ ТА ТИП ВЗАЄМОДІЇ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Войтович В.С.
Мандрона М.М., канд. техн. наук
Львівський державний університет безпеки життєдіяльності

Honeypot використовується в області комп'ютерної та мережевої безпеки. Це ресурс, який призначений для атаки і скомпрометування, щоб отримати більше інформації про зловмисника і його методи нападу. Він також може бути використаний для залучення та переадресації зловмисника в реальні системи. Метою цієї роботи є показати можливості honeypots та їх використання для захисту комп'ютерних мереж.

У порівнянні з системою виявлення вторгнень, honeypots має велику перевагу, – вони не створюють помилкові сповіщення, оскільки кожен трафік є підозрілим, тому що немає продуктивних компонентів, які працюють в системі. Цей факт дає змогу системі записувати кожен байт і до корелювати ці дані з іншими джерелами, щоб намалювати картину атаки і зловмисника [1].

Технологія honeypot має на увазі надання зловмисникові доступу до свідомо уразливому ресурсу. Після того як зловмисник отримає доступ, він буде робити ті чи інші дії, очікуючи відповідної реакції від системи. Залежно від того, як буде проводитися взаємодія системи і зловмисника, можна виділити два різних типи систем honeypot [2]:

- Високоінтерактивні системи (повністю імітують поведінку реальної системи);
- Низькоінтерактивні системи (володіють обмеженим функціоналом).

Високоінтерактивні системи найчастіше представляють собою окремий хост або пристрій, розташований всередині корпоративної мережі, але не використовується в інформаційних процесах. Таким чином, звернення ззовні до подібного ресурсу можна розглядати як порушення безпеки мережевої інфраструктури. Оскільки, такі системи надають зловмисникові повний функціонал реальних систем, то вони можуть також бути скомпрометовані і використані в якості допоміжних засобів для проникнення у реальну мережу та інших цілей, наприклад, формування ботнетів. Тому необхідно забезпечувати ізоляцію подібних систем. Такі системи, зазвичай, використовуються для отримання різної інформації про типи атак, мету порушника і потенційні вразливості у корпоративних інфраструктурах.

Низькоінтерактивні системи використовують різні механізми для імітації поведінки реальної системи. Це може бути, як операційна система, так і веб-сервер, сервер баз даних або навіть звичайний мережевий додаток.

Такі системи на відміну від високоінтерактивних використовують менше ресурсів, простіші в налаштуванні і не можуть бути використані порушником для здійснення атаки на реальні ресурси корпоративної мережі.

З іншого боку, вони легко виявляються порушником, через що такі системи більше підходять для протидії різним автоматизованих засобів, що використовуються порушниками, ніж для отримання будь-яких відомостей про них.

Наведемо основні переваги та недоліки кожного типу у вигляді таблиці 1.

Таблиця 1

Порівняння типів технологій Honeypot

	Низькоінтерактивні	***Високоінтерактивні***
Переваги	- простота настройки; - безпеки.	- повне функціонування; - складно виявити; - багато корисної інформації.
Недоліки	- легко виявити; - мало корисної інформації.	- складність розгортання і налаштування; - загроза безпеки.

Також існують системи, які складно віднести до того чи іншого класу. З одного боку, вони надають порушнику повний функціонал того чи іншого сервісу, а з іншого не виробляють ніяких «реальних» дій. Такі системи називають середньоінтерактивними [3].

Висновок: у даний час найбільшого інтересу викликаю високоінтерактивні динамічні honeypot-системи, оскільки із завданнями низькоінтерактивних систем справляються інші елементи корпоративної мережі: мережеві сканування успішно запобігаються міжмережевими екранами і системами виявлення та запобігання вторгнень, а також правильною конфігурацією елементів мережі, а інформація про конкретні дії зловмисника, зроблених для здійснення доступу у корпоративну мережу, надають набагато більшу цінність, ніж інформація про факт проникнення у мережу, яка також може бути отримана від міжмережевих екранів і засобів виявлення вторгнень.

Література:

1. The Honeynet Project [Електронний ресурс]. – Режим доступу: https://www.honeynet.org, вільний;

2. N. Provos, T. Holz. Virtual Honeypots: From Botnet Tracking to Intrusion Detection – Addison Wesley Professional, 2007;

3. Intrusion Detection FAQ: What is a Honeypot? [Електронний ресурс]. – Режим доступу: https://www.sans.org/security-resources/idfaq/honeypot3.php, вільний;