УДК 004.77

ПРОБЛЕМИ ВИКОРИСТАННЯ ВИСОКОІНТЕРАКТИВНИХ HONEYPOT-СЕРЕДОВИЩ ПРИ ДОСЛІДЖЕННІ ХАРАКТЕРУ МЕРЕЖЕВИХ ВТОРГНЕНЬ

Маліній Ілля, Месюра Володимир

Вінницький національний технічний університет

Анотація

Honeypot-середовище є досить потужним інструментом для збору даних при дослідженні характеру мережевих вторгнень. Його застосування дозволяє відслідковувати поведінку шкодоносного програмного забезпечення всередині мережі, а у випадку високоінтерактивних Honeypot-середовищ стає також можливим вивчення його діяльності на серверах та десктопних системах. Розглядаються можливості ботнетів щодо виявлення таких середовищ, а також можливості створення низькоінвазивних випробувальних середовищ.

Abstract

The Honeypot environment is a powerful toolkit for gathering data for network intrusions research. Usage of such toolkit allows monitoring of the behavior of malware within network, and in case of high interaction Honeypot environments, it is also possible to observe its activities on servers and desktop systems. The ability of detecting such environments by botnets is reviewed, as well as opportunities of developing of low invasive testing environments.

Вступ

Використання Honeypot-середовищ, наряду з системами IDS, є одним із найбільш ефективних методів виявлення мережевих вторгнень. На відміну від останніх, даний метод дозволяє збирати більше інформації про діяльність наявного в мережі шкодоносного ПЗ. Нині існує досить багато програмних реалізацій даного методу. Подібні рішення знаходять застосування як у виробничому середовищі, так і в дослідницьких цілях.

Досить використовуваною програмною реалізацією даного методу являється Honeyd [1]. Дана служба дозволяє досить швидко розгортати та конфігурувати потрібну кількість віртуальних мережевих хостів. Функціонал даного програмного забезпечення можливо розширювати за допомогою скриптів. Honeyd дає можливість створювали лише низькоінтерактивні середовища. Серед заявлених переваг досі є актуальними виявлення багатьох відомих та невідомих мережевих атак. Однак з розвитком технологій віртуалізації та контейнеризації, а також підвищення рівня їх доступності, на базі них з'явилось чимало більш багатих функціоналом альтернатив.

У написаній раніше статті [2] описується створення високоінтерактивного Honeypot-середовища для тестування ПЗ, яке не являється шкодоносним та використання у навчальних цілях. Як і в статтях [3, 4], у ній приділялась увага проблемам виявлення ознак Honeypot-середовища атакуючою стороною. Саме тому приділено більше уваги цим проблемам у контексті можливостей сучасних систем віртуалізації, а також побудови на їх базі високоінтерактивних Honeypot-середовищ. За ціль даного дослідження ставиться пошук методів створення низькоінвазивних Honeypot-середовищ, за допомогою яких стане можливим збір даних про мережеві вторгнення зі сторони ботнетів, які проводять ретельну перевірку середовищ інфікування.

Огляд проблем

З розвитком технологій віртуалізації та контейнеризації їх досить швидко стали впроваджувати в високоінтерактивних Honeypot-середовищах як основний інструмент розгортання. Шкодоносне ПЗ сучасних ботнетів в ході зараження нової системи виконує

ряд перевірок встановленого апаратного та програмного забезпечення [3]. Раніше відзначалось, що шкодоносне ПЗ припиняло процес зараження при виявленні ознак віртуальної машини [3]. Нині з розвитком ботнетів інфікування контейнера або віртуальної машини відбувається лише при наявних ознаках відлагоджувачів [5] або інших програм, що виконують перехоплення трафіку або перехоплення системних викликів. Боти деяких ботнетів не проводили інфікування систем GNU/Linux, де здійснювалась робота з файловою системою debugfs або пересилання телеметрії Honepot-сервісом [6,7,8,9,10].

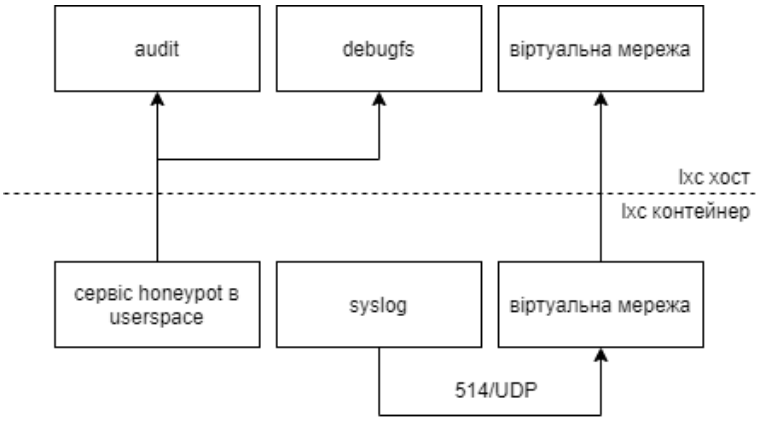

Рисунок 1 – Передача відлагоджувальних повідомлень на хостову систему

Серед основних причин ігнорування Honeypot-хостів було виділено наступні:

– Віддалене логування. Централізований запис логів перешкоджає їх видаленню, оскільки вони знаходяться на віддаленій системі. Для підтримки присутності багато видів серверного шкодоносного ПЗ видаляють повідомлення журналів, які пов'язані з їх діяльністю.

– Невідповідність TTL встановлених з'єднань із встановленою на сервері ОС [11]. Подібне може бути ознакою наявності мережевого екрану, на якому працює зворотній TCP-проксі або система виявлення вторгнень. Зазвичай це виявляється шляхом встановлення версії служб SSH та HTTPD при скануванні хоста. В деяких випадках ботнет може проігнорувати таку ціль.

– Наявність шкодоносного ПЗ інших ботнетів. У більшості випадків при інфікуванні конкуруюче шкодоносне ПЗ видаляється з системи, однак іноді процес може відбуватись і у зворотньому порядку [12].

– Наявність повідомлень з телеметрією стану системи. Подібно як і у випадку віддаленим логуванням активність агентів систем моніторингу може видати існування шкодоносного ПЗ в системі. Різні ботнети можуть проявлявляти різну поведінку у присутності агентів віддаленого адміністрування. Виключення складають випадки, коли подібні інструменти стають засобом проникнення шкодоносного ПЗ.

– Наявність відлагоджувальника у системі. Подібний випадок становить загрозу для ботнету попасти під виявлення, тому у більшості випадків зараження не відбувається або він просто видаляється якщо не є активним.

Для створення Honepot-середовища з використанням низькоінвазивних методів нарзі є відомими наступні методи: відслідковування системних викликів на рівні ядра та перехоплення пакетів на мережевому інтерфейсі ВМ.

Дані методи також піддаються виявленню ботнетами, однак за допомогою певних конфігурацій та патчів для системного ПЗ стає можливим зробити їх пристуність більш прозорою у складі Honepot-середовища.

Для відслідковування системних викликів існують різні підходи, основані на технологіях контейнеризації та віртуалізації. Підходи, що базуються на системах

контейнеризації, можуть використовувати засоби моніторингу ядра ОС GNU/Linux, такі як audit. Хоча на даний момент не існує способів ізолювати журнал ядра контейнера за допомогою cgroups [13], проте є можливість обмеження доступу до нього з непривілейованих контейнерів Docker/LXC за допомою параметра ядра kernel.dmesg_restrict.

Висновки

Розглянуто проблеми використання високоінтерактивних Honeypot-середовищ при дослідженні характеру мережевих вторгнень, зокрема можливості ботнетів у виявленні таких середовищ. Також було розглянуто можливості створення низькоінвазивних Honeypot-середовищ. В подальшому планується провести огляд методів створення таких середовищ.

Список використаних джерел

1. Provos N., Holz T. Virtual honeypots: from botnet tracking to intrusion detection [Text] / N. Provos, T. Holz – Pearson Education. – 2007. – 480 p.
2. Малініч І. П., Месюра В. І. Ін'єктивний метод отримання даних користувацького досвіду в ігрових симуляторах комп'ютерних мереж [Текст] / І. П. Малініч, В. І. Месюра // Вісник Вінницького політехнічного інституту. – 2019. – № 5. – С. 49-54.
3. Uitto J., Rauti S., Laurén S., Leppänen V. A Survey on Anti-honeypot and Anti-introspection Methods [Text] // Recent Advances in Information Systems and Technologies. Advances in Intelligent Systems and Computing – Springer, Cham – WorldCIST – vol 570. – 2017.
4. Krawetz N.. Anti-honeypot technology [Text] // IEEE Security & Privacy – vol. 2, no. 1. – 2004. – pp. 76-79.
5. Kuwatly I., Sraj M., Al Masri Z., Artail H.. A dynamic honeypot design for intrusion detection [Text] // The IEEE/ACS International Conference on Pervasive Services. – Beirut, Lebanon. – 2004. – pp. 95-104.
6. Mertens X. Analyze of a Linux botnet client source code [Електронний ресурс] / X. Mertens // Internet Storm Center of SANS Technology Institute – Режим доступу: https://isc.sans.edu/diary/Analyze+of+a+Linux+botnet+client+source+code/21305 – Назва з екрану. Дата публікації: 27.07.2016
7. Atluri A.C., Tran V. Botnets Threat Analysis and Detection [Text] – Springer. – 2017 – С. 15 – 27.
8. Know Your Enemy: Analysis of 24 Hours Internet Attacks [Електронний ресурс] / T. Britton, I. Liu-Johnston, I. Cugnière, S. Gupta, D. Rodriguez, J. Barbier, S. Tricaud // The Honeynet Project. – Режим доступу: https://www.honeynet.org/papers/kye-kyt/know-your-enemy-malicious-web-servers/ – Назва з екрану.
9. Know Your Enemy: Malicious Web Servers [Електронний ресурс] / C. Seifert, R. Steenson, T. Holz, B. Yuan, M. A. Davis // The Honeynet Project. – Режим доступу: https://www.honeynet.org/papers/kye-kyt/know-your-enemy-malicious-web-servers/ – Назва з екрану.
10. Know Your Enemy: Containing Conficker [Електронний ресурс] / T. Werner, F. Leder // The Honeynet Project. – Режим доступу: https://www.honeynet.org/papers/kye-kyt/know-your-enemy-containing-conficker/ – Назва з екрану.
11. Operating Systems Can be Detected Using Ping Command [Електронний ресурс] – Режим доступу: https://gbhackers.com/operating-systems-can-be-detected-using-ping-command/ – Назва з екрану.
12. linux.mirai/post.md [Електронний ресурс] // GitHub. – Режим доступу: https://github.com/0x27/linux.mirai/blob/master/post.md – Назва з екрану.
13. Hertz J. Abusing privileged and unprivileged linux containers [Text] / J. Hertz // NCC Group. Whitepaper 48. – 2016.