УДК 004.056

Ковцур М.М., кандидат технических наук,
доцент кафедры «Защищенные системы связи»
Санкт-Петербургский Государственный Университет Телекоммуникаций,
Российская Федерация, г. Санкт-Петербург
Ахрамеева К.А., кандидат технических наук,
доцент кафедры «Защищенные системы связи»
Санкт-Петербургский Государственный Университет Телекоммуникаций,
Российская Федерация, г. Санкт-Петербург
Юркин Д.В., кандидат технических наук,
доцент кафедры «Защищенные системы связи»
Санкт-Петербургский Государственный Университет Телекоммуникаций,
Российская Федерация, г. Санкт-Петербург
Акилов М.В.
студент 4 курс,
факультет «Инфокоммуникационные сети и системы»
Санкт-Петербургский Государственный Университет Телекоммуникаций,
Российская Федерация, г. Санкт-Петербург

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ HONEYPOT РЕШЕНИЙ ДЛЯ КОРПОРАТИВНЫХ СЕТЕЙ

Аннотация: *В статье анализируются тенденции в области применения сетевых технологий, использующих honeypot-решения для обнаружения и исследования различных атак и поведения нарушителя в целях обеспечения безопасности в корпоративных сетях.*

Ключевые слова: *корпоративные сети, облачные вычисления, Deception Technologies (технологии «обманки»), Honeypot-решение, безопасность инфокоммуникационных сетей, киберугрозы*

Annotation: *Trends in the sphere of network technologies with honeypot technologies use are analyzed to detect and explore different kinds of attacks and intruders behavior in order to ensure security in corporate networks.*

Key words: *corporate networks, cloud computing, deception technologies, honeypot technologies, infocommunication networks security, cyber threats.*

Назначение и перспективность применения технологий «обманки» в корпоративных сетях

Большинство современных центров защиты информации оснащены технологиями, фиксирующими инциденты безопасности [1-3]. Однако, современная ситуация с защитой периметра сети все чаще рассматривается специалистами с точки зрения времени, за которое злоумышленников обнаруживают внутри сети. Недостаточно найти и удалить нарушителя из сети. Требуется более полно изучить противника, а для этого нужна наиболее полная статистика его действий.

Так как действия нарушителя могут нести в себе угрозу, необходимо проводить изучение злоумышленника в имитированной среде, воспринимаемой им как естественная среда (оставаясь при этом незамеченными для него), где невозможно нанесение какого-либо ущерба [4-5]. При этом следует обеспечить защиту от обнаружения факта обмана, для увеличения времени пребывания злоумышленником в исследовательской среде, что может достигаться использованием технологий «обманки», которые выглядят весьма естественно, но являются приманками, содержат скрытые механизмы оповещения и др. [6].

Распределение ловушек и приманок целесообразно осуществлять по всей сети и на конечных точках, которые представляются информационными активами организации. Как только злоумышленник подключается к «среде обмана», выдается предупреждение, что с высокой точностью позволяет организации принять решение – либо быстро исключить нарушителя из сети, либо изучить его методы и поведение в контролируемой среде. Доказано [4], что использование технологий «обманки» сильно сокращает время пребывания

злоумышленника в среде до того, как он будет обнаружен средствами контроля безопасности.

Одним из эффективных направлений технологий «обманки» является использование Honeypot, которые привлекательно выглядят для киберпреступника, но не содержат важных данных, а только имитируют их наличие и возможность доступа. Иными словами, «обманка» с помощью Honeypot – проактивная защита, которая делает атаку более трудной для выполнения, и в то же время делает возможным нанесение ответного удара по злоумышленнику. В процессе взаимодействия с Honeypot атакующий раскрывает свои приемы, средства и возможности, может быть идентифицирован в дальнейшем при анализе массивов данных об аналогичных инцидентах [5]. Успешность применения технологий Honeypot-«обманки» в значительной степени зависит от того, насколько реалистично активы сети выглядят при попытке доступа извне, а также от того, насколько эффективно реализованы механизмы наблюдения и анализа происходящих в них событий.

В последнее время ряд исследователей склонны использовать термин Honeypot для обозначения совокупности использующих данный подход технологий, как концептуальное направление для различных прикладных решений.

Концепция Honeypot и сравнение типичных решений

Если рассматривать концепцию, как имитационную модель реального вычислительного процесса, то к любому программно-аппаратному решению на базе этой концепции применимо ограничение Тьюринга. Последнее требует применения рациональных подходов к реализации Honeypot-решений в контексте более конкретной задачи.

Так появились решения на базе Honeypot, которые разделяются по объектам, категориям и области применения в сети (таблица 1).

Таблица 1

Классификация Honeypot-решений по области применения

Технологические Решения	**Объект «обманки»**	**Категория**	**Хост**	**Сеть**
Fake Honeypot	Honeypot	Server	X	✓
Honeyentries	Table, data set	Database	✓	X
MTD	Topo,net.interf.,memory,arch	Versatile	✓	✓
Honeyword	Password	Authentication	✓	X
Honeyfile	(Cloud-)File	File system	✓	✓
Honeypatch	Vulnerability	Server	✓	✓
—	Memory	Server	✓	X
—	Metadata	File	✓	X
HoneyURL	URL	File	X	✓
Honeymail	E-Mail address	File	X	✓
Honeypeople	Social network profile	File	X	X
Honeyport	Network port	Server	X	✓
Decep. Web server	Error codes,Robot.txt	Server	X	✓
OS interf.	System call	Server	✓	X

Таблица отражает типичные технологические решения, составлена на основе анализа их функциональных возможностей и результатов тестирования, описанных в литературе с учетом задач и имитируемых объектов. Функциональные возможности Honeypot-продуктов могут расширяться, области применения пересекаться, в том числе вследствие специфики сетей [11].

Таким образом, на данный момент не существует абсолютно универсального решения, которое использует концепцию Honeypot. Каждое решение удовлетворяет лишь весьма ограниченному количеству задач. По мере усложнения сетей и вычислительных систем, увеличению числа возможных угроз, расширились задачи и для Honeypot. Их разработка стала циклическим

процессом, так как требует постоянного совершенствования для более эффективного привлечения злоумышленников. Таким образом, актуальной является задача разработки комплексного решения, которое могло бы сочетать в себе все преимущества существующих решений для выявления нарушителей, а также применение технологий больших данных и искусственного интеллекта для управления несколькими Honeypot одновременно.

Использованные источники:

1. Покусов В.В. Особенности взаимодействия служб обеспечения функционирования информационной системы // Информатизация и связь. 2018. № 5. С. 51–56.

2. Buinevich M., Fabrikantov P., Stolyarova E., Izrailov K., Vladyko A. Software Defined Internet of Things: Cyber Antifragility and Vulnerability Forecast // Proceedings of the 11th International Conference on Application of Information and Communication Technologies (AICT, Moscow, Russia, 20–22 September 2017). Piscataway, NJ: IEEE, 2017. PP. 293–297. DOI:10.1109/ICAICT.2017.8687021

3. Kotenko I., Kuleshov A., Ushakov I. Aggregation of elastic stack instruments for collecting, storing and processing of security information and events // Proceedings of the SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI, San Francisco, USA, 4–8 August 2017). Piscataway, NJ: 2017. DOI:10.1109/UIC-ATC.2017.8397627

4. Котенко И.В., Левшун Д.С., Чечулин А.А., Ушаков И.А., Красов А.В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3(27). С. 29–38. DOI:10.21681/2311-3456-2018-3-29-38

5. Котенко И.В., Ушаков И.А., Пелёвин Д.В., Овраменко А.Ю. Гибридная модель базы данных NoSQL для анализа сетевого трафика // Защита информации. Инсайд. 2019. № 1(85). С. 46–54.

6. Котенко И.В., Ушаков И.А. Использование технологий больших данных для мониторинга инцидентов информационной безопасности // Юбилейная XV Санкт-Петербургская Международная Конференция «Региональная Информатика (РИ-2016)». СПб.: СПОИСУ, 2016. С. 168–169.

7. Красов А.В., Петрив Р.Б., Сахаров Д.В., Сторожук Н.Л., Ушаков И.А. Масштабируемое Honeypot-решение для обеспечения безопасности в корпоративных сетях, «Труды учебных заведений связи». 2019. Т. 5. № 3. С. 86-97.

8. Ушаков И.А., Котенко И.В., Крылов К.Ю. Анализ методик применения концепции больших данных для мониторинга безопасности компьютерных сетей // IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2015)». СПб.: СПОИСУ, 2015. С. 75–76.

9. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой Сахаров Д.В., Ковцур М.М., Бахтин Д.В.// Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 22-31

10. Обзор способов человеко-компьютерного взаимодействия для сетевой безопасности Виткова Л.А., Десницкий В.А., Жернова К.Н., Чечулин А.А. //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) сборник научных статей VIII Международной научно-технической и научно-методической конференции: в 4 т.. 2019. С. 218-223.

11. Fraunholz D., Schotten H.D. Defending Web Servers with Feints, Distraction and Obfuscation // Proceedings of the International Conference on Computing, Networking and Communications (ICNC, Maui, USA, 5–8 March 2018). Piscataway, NJ: IEEE, 2018. DOI:10.1109/ICCNC.2018.8390365.