УДК. 004.056

HONEYPOT КАК СРЕДСТВО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Череватенко Д.Р., Торбеева М.В.
Государственный ВУЗ “Национальный горный университет”, nmu.org.ua, dencherevatenko@ya.ru

В докладе рассматривается технология Honeypot: её суть, типы и области применения. В результате анализа выделены основные достоинства и недостатки данной технологии.

Ключевые слова: Honeypot, информационная безопасность, злоумышленник.

Современные средства безопасности позволяют в значительной мере противостоять стандартным направлениям атак, но они не защищают от малоизвестных атак, защиты от которых может и не быть. Решением этой проблемы может стать внедрение в комплекс средств защиты скрытых ловушек. Данная технология является своего рода инструментом, который можно настроить для решения широкого круга задач обеспечения информационной безопасности на предприятии. Honeypot может стать дополнением существующей системы безопасности предприятия и быть средством по сбору важной для системы защиты информации.

Средства Honeypot отличаются от классических средств обеспечения безопасности, таких как межсетевые экраны или системы обнаружения вторжений, тем, что они не призваны решать какую – либо конкретную задачу. Напротив, Honeypot – гибкое средство, которое может быть применено в различных ситуациях. Например, средства Honeypot позволяют обнаруживать и предотвращать атаки. По сути, Honeypot включают в себя функциональность практически всех средств обеспечения безопасности.

В зависимости от степени взаимодействия со злоумышленником средства Honeypot делятся на 3 типа:

1. Слабого взаимодействия;
2. Среднего взаимодействия;
3. Сильного взаимодействия.

Основное различие представленных типов взаимодействия состоит в сложности их установки, использования и поддержки, а также в уровнях протоколирования, имитации и рисках. Так средства слабого взаимодействия легко устанавливаются и просты в использовании, но они менее продуктивны. В то время как средства сильного взаимодействия обладают высоким уровнем протоколирования и имитации, однако они являются куда более сложными в использовании. Кроме того, использование такого типа Honeypot влечет за собой более высокий риск обнаружения и компрометации.

Областью применения средств Honeypot может быть как информационная система предприятия, где они выступят в качестве составляющих частей системы безопасности, так и научные исследования, где они станут платформой для изучения действий злоумышленника. Honeypot может дать точную информацию в быстром и легком для понимания формате. Это упрощает анализ и уменьшает время реакции. Honeypot может использоваться для уточнения своего собственного значения и инвестиций в другие ресурсы безопасности.

Технологии Honeypot предоставляют аналитикам такие преимущества, как:

1. Сбор содержательной информации;
2. Нетребовательность к системным ресурсам;
3. Наглядность необходимости использования средств информационной безопасности.

Однако, наряду с этим, средства Honeypot обладают и рядом недостатков:

1. Ограниченная область видения;
2. Возможность раскрытия Honeypot злоумышленником;
3. Риск взлома Honeypot и атаки узлов посторонних организаций.

Тем не менее, при правильной установке и настройке эти недостатки оказываются несущественными, а применение самой технологии Honeypot позволяет разрешить такие задачи информационной безопасности, как:

1. Уточнение моделей угроз и нарушителя;
2. Оправдание затрат на систему информационной безопасности предприятия;
3. Отслеживание методов, используемых нарушителем;
4. Определение новых средств воздействия злоумышленников.

Таким образом, следует отметить, что Honeypot является гибкой технологией, которая может быть применена во множестве ситуаций. Как средства осуществления безопасности Honeypot имеют целый ряд преимуществ и могут послужить прекрасным дополнением системы защиты, выполняя такие функции как обнаружение, предупреждение и противодействие несанкционированной деятельности в сети. А также Honeypot могут найти своё применение как важное средство по исследованию новых методов, средств и мотиваций злоумышленников.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Lance Spitzner. Honeypots: Tracking Hackers. Addison Wesley, 2002.
2. Honeypots: Monitoring and Forensics, 2002.
3. Lance Spitzner. Dynamic Honeypots, 2003..
4. The Honeynet Project. Know Your Enemy: Learning about Security Threats, 2003.
5. http://www.compdoc.ru/secur/internet/honeypot