УДК 004.56

ПОВЫШЕНИЕ БЕЗОПАСНОСНОСТИ СЕТИ С ПОМОЩЬЮ ИНСТРУМЕНТА HONEYPOT

Юмашева Е.С. (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)

Научный руководитель – д.т.н., профессор Гатчин Ю.А.

(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)

В данной работе представлен подход к развертыванию системы honeypot во внутренней сти, которая является упреждающей мерой безопасности и позволяет обнаруживать злоумышленника, а также отслеживать его действия в сети. На основании собранных данных системный администратор изучает стратегии злоумышленника и определяет перечень средств, с помощью которых был нанесен «удар».

Введение. Одним из способов увидеть, как именно хакер взламывает «живую» сеть, а также узнать потенциального злоумышленника, является развертка honeypot. Это система вашей сети, которая действует как приманка и заманивает потенциальных хакеров. Honeypots не содержит никаких «живых» данных или информации, но может содержать ложные. Кроме того, honeypot должен препятствовать доступу злоумышленника к защищенным областям действующей сети.

Правильно настроенная система должна иметь много функций реальной производственной системы. Это может включать в себя графические интерфейсы, предупреждения о входе в систему, поля данных и.т.д. Злоумышленник не должен быть в состоянии обнаружить, что он находиться в системе honeypot, отслеживающей его действия.

Преимущества системы. У многих организаций возникает вопрос, для чего именно они должны тратить финансовые средства и временные ресурсы на создание системы, привлекающей хакеров. Самая значимая ценность honeypot основана на информации, которую он получает и может немедленно предупредить. Данные, которые поступают в приманку и покидают её, позволяют сотрудникам службы безопасности собирать информацию, недоступную в системе обнаружения вторжений (IDS). Любые попытки получить доступ к системе сопровождаются немедленным оповещением.

IDS требует опубликованных баз сигнатур для обнаружения атаки, тем самым часто атака неизвестная в данное время становиться необнаруженной. Honeypot s, с другой стороны могут обнаруживать уязвимости на основе поведения злоумышленника, о котором может быть неизвестно (эксплойты нулевого дня).

Данные, собранные honeypot, могут быть использованы для улучшения других технологий информационной безопасности. Система предоставляет возможность соотнесения своего системного журнала, с другими системными журналами, IDS оповещениями и журналами Firewall. Это позволяет получить исчерпывающую картину подозрительной активности в организации и позволит настроить более релевантные оповещения, которые позволят сократить количество ложных срабатываний.

Еще одним преимуществом является то, что чем больше времени проведено в honeypot, тем меньше времени уходит на производственную систему.

Проектирование и эксплуатация приманки. Существует множество операционных систем и сервисов, которые может использовать honeypot. Honeypot с высокой степенью взаимодействия может обеспечить полную систему производственного типа, с которой атакующий может взаимодействовать.

На другом конце находится приманка с низким уровнем взаимодействия, имитирующая определенные функции производственной системы. Они более ограничены, но и полезны для получения информации на более высоком уровне. Однако для развертывания и настройки такой системы требуется большое количество времени.

Важно настроить правильное оповещение honeypot. Должны быть журналы для всех устройств, входящих в систему, отравленные на централизованный сервер журналирования, а персонал службы безопасности должен быть оповещен всякий раз, когда злоумышленник входит в среду. Это позволит сотрудникам отслеживать злоумышленника и следить за безопасность производственной среды.

Важно также, чтобы ваша система была привлекательной для потенциального злоумышленника. Она не должна быть такой же безопасной, как и ваша производственная система. Должны присутствовать сканеры портов, учетные записи пользователей и различные системные файлы. Пароли к фальшивым учетным записям должны быть слабыми, а некоторые уязвимые порты должны остаться открытыми. Это даст толчок злоумышленнику перейти в среду honeypot.

Хакеры чаще всего атакуют менее безопасную среду, прежде чем перейти к среде с более сильной защитой. Что позволяет сотрудникам службы ИБ узнавать, как именно хакеры обходят стандартные средства защиты, и после этого могут вносить любые необходимые изменения.

Развернуть Honeypot можно как физически, так и виртуально. В большинстве случаев лучше разворачивать виртуальную среду, поскольку она более масштабируема и проста в обслуживании. Появляется возможность иметь тысячи приманок на одной физической машине, плюс виртуальные приманки дешевле и более доступны.

Защита внутренней сети от внутренних угроз. Согласно исследованию Cyber security Intelligence Survey, IBM обнаружила, что 60% всех атак были произведены инсайдерами. Honeypot должна быть развернута во внутренней сети, и только минимальное количество сотрудников должно знать о системе. Внутреннее развертывание предпочтительнее внешнего из-за большого числа атак, осуществляемых инсайдерами, и того факта, что многие хакеры предпочитают устанавливать серверы управления и контроля для связи с скомпрометированными серверами во внутренней сети.

Honeyd - инструмент с открытым исходным кодом, используемый для создания honeypots. Это домен, который можно использовать для создания множества виртуальных хостов. Появляется возможность настроить каждый хост по-разному и запускать их на различные сервисы. Их можно настроить для работы в разных ОС. Например, настроить реальные HTTP-серверы, FTP-серверы и запустить приложения Linux. Что позволяет моделировать различные топологии сети.

На данный момент honeypots используются главным образом исследователями, чтобы изучить тактику и методы нападающих. Но, как было сказано выше, они очень эффективны для специалистов ИБ. Стоит обратить внимание на использование таких систем в качестве проактивного способа защиты своей сети.

Юмашева Е.С. (автор) Подпись

Гатчин Ю.А. (научный руководитель) Подпись