Эссе на тему “ HONEYPOTS “

Кузьмина Олега 914 группы

Вместе с совершенствованием компьютеров постоянно меняется характер преступлений и компьютерной безопасности. Большая часть компьютерных инцидентов, связанных с нарушением безопасности систем, так или иначе нарушают законы, поэтому считаются преступлениями (включая кражу информации, промышленный шпионаж, неавторизованный доступ, продажу наркотиков, детскую порнографию и т.д.).

Одним из наиболее эффективных способов борьбы с атакующими является выявление конкретных виновников инцидентов! Многие компании становятся жертвами компьютерных атак, включая вымогательство, кражу интеллектуальной собственности и других сетевых преступлений. Многие атакующие надеются на свою неуязвимость и безнаказанность. Они могут действовать из других стран, заметать следы своей работы, проходить через множество промежуточных систем для скрытия своего местоположения и не предполагают выдачу в случае обнаружения. Они надеются на технические средства и недостатки в законодательстве, причисляя себя к "элите" хакерского движения. Действительно, во многих законах предполагается "только поиск дураков", но предварительные защитные мероприятия и обучение методам реакции на инциденты позволяют поймать даже самых квалифицированных атакующих.

Кроме непосредственной защиты компьютерных систем от вторжений и атак весьма полезно проводить обнаружение попыток неавторизованного доступа. Обычно с этой целью применяется некоторая система обнаружения вторжений IDS (Intrusion Detection System), но последнее время даже отдельные компании стали использовать средства, ранее применявшиеся только экспертами по компьютерной защите. Одним из таких средств стал метод honeypots ("ловли на живца"). Стоит заметить , что для этого термина нет пока утвержденного русского перевода . В моем же представлении - это система , предназначенная для изучения стратегии (тактики) хакеров , которую они используют для проникновения в чужие системы . В идеале , хорошо настроенная система honeypot не позволяет хакеру определить , что за ним следят. Существуют различные способы , как этого добиться.

Непосредственное изучение методов проникновения помогает лучше настроить свои сети для защиты от реальных атак , либо когда для потенциальных взломщиков в частной сети специально организуется хост (сайт) , который только и ждет , чтобы его взломал какой-нибудь нарушитель . Обычно такой сайт моделирует определенную системную архитектуру (хотя и не обязан иметь ее в наличии) , либо некоторую службу , например почтовую службу SMTP .

Разобьем программы honeypots на 2 широкие катагории : производственные и исследовательские . Цель производственных honeypots – помочь уменьшить риск незаконного доступа в компьютеры различных организаций и повысить их уровень безопасности . Их задача состоит в том , чтобы обнаруживать и иметь дело с незаконными вторжениями “плохих парней” . Обычно , коммерческие организации используют эти программы для помощи в защите своих сетей . Вторая же категория – исследовательские программы honeypots разработаны для получения и сбора информации о хакерах . Эти программы используются для исследования угроз от хакеров , с которыми могут столкнуться разные организации , и как лучше противостоять этим угрозам . Такие программы не используют обычные компании , этим уже занимаются специализированные организации , институты и правительство.

Программы honeypots являются инструментом безопасности и они имеют ряд преимуществ и недостатков . Достоинство программ honeypots состоит в их простоте. Одной из больших проблем в безопасности это найти нужную тебе информацию в потоке мегабайт данных, и программы honeypots могут предоставить эту информацию быстро и в простом , понятном формате. Специальные log – серверы не всегда могут собирать информацию о происходящем в сети , пропуская некоторые события , из-за перегрузки сети или других факторов . Программы honeypots не сталкиваются с этой проблемой , они только складывают и хранят информацию , которая поступает к ним . Но у этих программ есть определенные недостатки . Например , они становятся только бессмысленной тратой ресурсов , если не происходит никакой атаки .Также они могут

предоставить риск для вашей сети . То есть , подключая дополнительнительное оборудование к сети , мы предоставляем хакеру дополнительные платформы для его действий и последующего запуска новых атак . Этот риск зависит от того , как мы настроим и подключим honeypot , потому что мы не заменяем уже существующий механизм защиты , а только улучшаем уже существующую систему защиты .

Рассмотрим , как мы можем применить программу honeypot для защиты .
Настраиваем стандартный хост, им может быть Linux , Solaris , NT или другая операционная система (ОС) . Не делаем ничего особенного с системой , настроим ее как обычно , чтобы затруднить распознавание хакером приманки . Подключите ее к Internet и просто ждем . Рано или поздно кто-нибудь найдет ее и атакует . Кто-нибудь получит на этой системе права root'a , что и является нашей целью , причем процесс получения этих прав мы подробно зафиксируем..

Первый вопрос , возникший после настройки хоста и подключения его к Internet состоял в том, каким образом мы будем следить за действиями атакующего и фиксировать их. Вторая проблема: как настроить систему так , чтобы она давала сигнал о начале атаки . И последнее , каким образом остановить хакера , чтобы он не использовал захваченную систему для атаки других . Все эти проблемы решаются , если установить honeypot за брандмауэром (межсетевой экран , firewall) . Первое , большинство брандмауэров собирают информацию и статистику его трафика, проходящего через них. Он будет представлять первый уровень ведения логов активности хакера. Второе, большинство брандмауэров имеют возможность подачи соответствующего сигнала о идущей атаке(на примет. Сканирование сети). Поскольку начально о нашей приманке никому не известно , то можно предположить , что большинство входящих пакетов генерируется атакующим . Если есть исходящий трафик из honeypot , то , наиболее вероятно, что honeypot взломана . Третье , брандмауэр может контролировать как входящий , так и исходящий трафик . Поэтому можно настроить его таким образом , чтобы для входящего трафика препятствий не было , я выходящий был ограничен таким образом , чтобы хакер не мог использовать нашу систему как плацдарм для атак на другие.

Реальный трюк заключается в том , как фиксировать действия хакера так , чтобы он не знал об этом . Первое , вы не должны зависеть от единственного источника информации . Что-нибудь может пойти не так, логи могут быть почищены, поэтому желательно вести логи на нескольких уровнях . Если что-нибудь пойдет не так на одном уровне , то у вас всегда есть дополнительные источники информации на других .

Третий уровень слежения - использование программу сыщика (snifer) . Поскольку honeypot изолирована с помощью брандмауэра в нашем случае , то можно следить за всем проходящим трафиком . Преимущество снифера заключается в том , что он фиксирует нажатия клавиш нажатия клавиш и то , что выдает система на экран хакеру . Поэтому в точности можно восстановить его действия . Недостаток применения снифера : хакер может свести его пользу на нет , используя , например , ssh (при наличии на honeypot соответствующих служб , сервисов) .Также продвинутый пользователь может сам обмануть программу сыщика (snifer) , которая попытается из Интернета отследить действия этого пользователя , открытые для доступа адреса , либо какие-нибудь иные информационные ресурсы , будто бы открытые для атаки .

Помните , что наша цель - изучение стратегии (тактики) хакеров , а не их поимка . Дело в том , что выявление IP – адресов или персональной информации атакующего систему человека по закону многих стран считается хакерским действием и может проводиться только специальными , уполномоченными на это , государственными службами (полиция , милиция , ФСБ , ЦРУ) . Если частная компания или отдельный человек сам попытается ловить хакеров взломавших его систему , то такое юридическое лицо само становиться хакером , и его действия считаются незаконными во многих странах мира. Кроме того , отслеживание действия хакеров обычно требует обращения в так называемые промежуточные организации (провайдеры Интернета , владельцы Интернет сайтов, владельцы служб хостинга или владельцы интерактивных служб , например служб обеспечения анонимности) . Нам необходимо привлечь хакера , проследить за его действиями , затем , как бы случайно, избавиться он него так , чтобы он ни о чем не догадался. Для привлекательности , для доменных имен хостов , можно использовать названия типа

ns1.example.com (name server) , mail.example.com (mail server) или intranet.example.com (internal web server) .

Что мы предпринимаем , после того как хакер получает права root'a ? Обычно , еще несколько дней можно следить за его действиями . Однако , надо быть осторожным , так как хакер может выяснить , что находится в honeypot , что может иметь плохие последствия . После того как мы выяснили все , что могли , можно избавиться от хакера сделав новый honeypot или отключая систему от Internet . Убираем backdoor'ы , оставленные хакером и снова ее подключаем , уже по фикся уязвимости , через которые были получены права root'a (или менее приоритетный доступ) , чтобы в следующий раз хакер использовал уже другие дыры .

Кроме моделирования наживки в реальных сетях можно использовать специальные сети , предназначенные исключительно для анализа вторжений . Такие сети позволяют проследить тенденции в хакерском сообществе . Среди специальных сетей такого рода можно отметить DShield.org, myNetWatchman, DeepSight Analyzer от Symantec или XFTAS (X-Force Threat Analysis Service) от ISS (Internet Security Systems). Это так называемые сети анализа угроз (threat-analysis network). В любом случае предполагается использования ПО на клиентской стороне для сбора статистических данных о неавторизованных действиях как опытных злоумышленников , так и только начинающих .

Теперь когда рассказано о различных видах программ honeypots , стоит рассмотреть несколько примеров этих программ . Стоит заметить , что из большого большинства таких программ вы не найдете какие-либо две , которые будут похожи по своим возможностям , функциям и степени скрытности . Однако чем программа более сложная по своей функциональности , тем больше шансов у злоумышленника заметить и использовать ее в дальнейших своих противоправных делах . Из разнообразного количества программ honeypot
стоит выделить BackOfficer Friendly, Specter, Honeyd, homemade honeypots, Mantrap, and Honeynets.

BackOfficer Friendly (или BOF как ее обычно называют) очень простая и высоко полезная программа разработанная Маркусом Ранумом (Marcus Ranum) . Она является очень распространенной из-за своей простоты для пользователей . BOF установлена на большинстве машин работающих с ОС Windows . Всё что она может , это эмуляция установленных популярных служб (таких как http, ftp, telnet, mail) и дальнейшее прослушивание и записывание обращений к портам . Таким образом можно определить атаку или неавторизированный доступ в вашу систему. Хотя BOF может обеспечивать работу только ограниченного числа портов , но эти порты как раз и являются обычно для сканирования и последующей атаки запущенных приложений.

Specter - это уже коммерческая программа , которая тоже как и BOF , предназначена не для профессионалов , а для продвинутых пользователей . Правда в ней уже эмулируется работа большего числа служб и программ , а также может эмулировать работу некоторых ОС . Как и BOF, она проста в работе и представляет собой малый риск , так как на рабочей машине будет хакеру будет подменена настоящая ОС - несуществующей , с которой ему трудно будет взаимодействовать . Также Specter поддерживает ряд различных видов сигналов оповещения вторжения и механизмов записи действий нападающего. Одним из уникальных свойств этой программы является то , что она в свою очередь не только записывает действия нападающего на вашей системе , но и параллельно получает информацию о преступнике используя DNS lookup , а также сканируя порты нападающего . Правда нападающий таким образом может определить , что за ним уже следят .

Homemade Honeypots - эта программа уже предназначена для профессионалов по защите . Она уже вполне может определить и справиться с атакой "бомба" , чего не могут делать предыдущие программы . Также она может справлять с некоторыми червями , например W32/Leaves Worm . Эмулирует сложную работу Windows NT и Win2000 на вашем компьютере . Также определяет атаки sendmail spammers.

Ну и наконец , самая популярная профессиональная программа Honeyd созданная Niels Provos. Стоит вначале заметить это Open Source honeypot , что дает ей большую популярность , но не

стоит забывать и о ее функциональной стороны. На данный момент она считается чрезвычайно полезной программой .Разработанная для работы на компьютерах ,работающих под системой Unix, она может эмулировать работу более 400 различных операционных систем ,с разными настройками , и около 1000 различных компьютеров - и всё это одновременно ! Honeyd предоставляет несколько полезных новых свойств. Во-первых , она не только эмулирует работу операционных систем на уровне приложений , но и работу ОС на уровне IP стека . Это означает , сто если кто-то использует программу Nmap , то он увидит , что как службы , так и IP стек ведут себя работая под эмулируемой рабочей ОС . Во-вторых , Honeyd может эмулировать работу 1000 разных компьютеров одновременно . То есть , она может присвоить тысяче компьютерам различные IP адреса. В-третьих , она распространяется совершенно бесплатно .

Системы honeypots являются очень мощным инструментом для изучения методов работы представителей хакерского сообщества. Их правильная настойка позволяет "из первых рук" получить ценную информацию о практических способах проникновения в чужие системы .

Литература :

1. М.Кузьмин "Honeypot и сети анализа трендов" - сайт www.itunion.ru
2. Lance Spitzner "Honeypots - *Definitions and Value of Honeypots* "