1 Начало

Как провести аудит законно?

Конечно же, любой профессионал в области информационной безопасности хочет заниматься любимым делом на законных основаниях. Но взламывать системы, которые ты же и конфигурировал, не всегда бывает интересно. Гораздо приятнее помериться силами с профессионалами, находящимися по другую сторону баррикады. Попробовать на прочность чужую сеть.

Чаще всего такие люди являются частью команды, проводящей комплексный аудит безопасности информационных систем предприятий. Но иногда они устраивают тесты на проникновение и в индивидуальном порядке.

Чтобы быть уверенным в правильности и законности своих действий, профессионал должен соблюдать следующие правила:

- получить от клиента письменное разрешение на проведение тестов на проникновение или аудита ИС;
- соблюдать соглашение о неразглашении, особенно в случае, если во время тестов был получен доступ к конфиденциальной информации;
- никакая информация, полученная во время работы с клиентом, никогда не должна стать известной другим лицам;
- проводить все тесты, согласованные с клиентом, и никакие другие. Например, тесты, нацеленные на проверку устойчивости систем к типу атак «отказ от обслуживания», должны проводиться только по предварительному согласованию и в строго обозначенный временной интервал.

Обычно аудит информационных систем проходит в несколько этапов.

1. Встреча с клиентом, обсуждение целей и средств.
2. Подписание договора о неразглашении информации.
3. Сбор группы участников аудита и подготовка расписания тестов.
4. Проведение тестов.
5. Анализ полученных результатов и подготовка отчета.
6. Передача отчета клиенту.

Методология взлома

Аудит информационной системы можно условно разделить на пять этапов, которые идут последовательно, один за другим:

1. **Сбор информации (Google, WWW, DNS)**;
2. **Сканирование системы (ping, port scanning)**;
3. **Получение доступа (эксплуатация уязвимости)**;
4. **Закрепление в системе (backdoor)**;
5. **Скрытие следов пребывания (очистка лог-файлов, rootkit)**.

Данный цикл может повторяться итеративно. Например, в случае, когда мы получили доступ к серверу, через который можно проникнуть во внутреннюю сеть. Тогда мы сначала собираем информацию о внутренней сети, а затем используем ее для дальнейшего проникновения.

Данная методология является всего лишь приблизительной. Обычно у людей, занимающихся вопросами информационной безопасности, есть своя методика, основанная на их специфических требованиях и уровне профессиональной компетенции. Мы рекомендуем вам также ознакомиться с OSSTM — Open Source Security Testing Methodology. Это открытый стандарт, в котором рассматривается методология аудита безопасности ИС-систем.

Этап первый: пассивный и активный сбор информации

Прежде чем начать активный взлом системы, нам надо собрать как можно больше информации о нашей цели. Можно сказать, что от того, насколько хорошо мы будем знать нашу цель, напрямую будет зависеть успех или провал всего мероприятия. Это самый важный этап аудита системы, на который чаще всего уходит большая часть времени.

Условно сбор информации делят на активную и пассивную фазы. Во время пассивной фазы наша «цель» не знает о том, что мы начали сбор информации. На данном этапе мы используем информацию только из отрытых и общедоступных источников, таких как поисковые системы и базы данных NIC. Также к пассивному сбору информации можно отнести снифинг — когда мы просто перехватываем всю приходящую на наш сетевой интерфейс информацию и при этом ничего сами в сеть не посылаем.

Под активным сбором информации подразумевается непосредственное взаимодействие с системой. И скорее всего, данная активность будет занесена в журнал аудитации целевой системы.

К данной фазе можно отнести сканирование портов, определение работающих сервисов и их версий, а также определение версии операционной системы, под управлением которой работают данные сервисы.

Этап второй: сканирование системы

Предположим, что, используя добытую на первом этапе информацию, мы получили из открытой базы данных RIPE диапазон IP-адресов целевой организации. После этого мы начинаем сканирование всей подсети предприятия.

На данном этапе чаще всего используются:

- сканеры открытых портов;
- ICMP-сканеры;
- SNMP-сканеры;
- сканеры уязвимостей и т. д.

Во время данного этапа аудитор может получить следующую информацию:

- имена компьютеров;
- версию операционной системы;
- запущенные сервисы и их версии;
- IP-адреса;
- учетные записи пользователей и т. д.

Этап третий: получение доступа

После получения информации в результате предыдущего этапа мы можем использовать ее для проникновения в систему. Например, мы узнали, что на одном из хостов установлен IIS. Используя версию и название сервиса, можно найти уязвимость, а затем и поэксплуатировать ее.

Одни из самых популярных методов — перехват сессии, переполнение буфера и отказ от обслуживания.

Этап четвертый: закрепление в системе

Поскольку редко получается проникнуть в систему с наскока, мы хотим использовать повторно полученный однажды доступ. Нам нужна возможность продолжить начатое ранее тестирование, не прибегая к очередному взлому той же самой системы.

Самые популярные методы сохранения доступа к системе — установка троянских коней, backdoor'ов и rootkit'ов.

Этап пятый: скрытие следов пребывания

Итак, мы получили доступ к обозначенной системе и контролируем ее. Разумеется, мы не хотим, чтобы кто-то из ИТ-персонала компании заметил наше присутствие. В противном случае мы можем потерять доступ не только к полученной системе, но и к сети в принципе.

Чаще всего стирают следы присутствия из журналов аудитации, а также события из базы данных IDS (системы обнаружения атак).

Резюме

Помните, что любой аудит информационной системы по сути представляет собой ее взлом, разница только в том, насколько легитимны проводимые мероприятия. Чтобы ваши действия были законными, необходимо получить письменное согласие заказчика. Обязательно обсудите заранее все действия, методы и риски и зафиксируйте их документально.

Проведение аудита осуществляется в несколько основных этапов:

- Планирование и получение согласия.
- Пассивный сбор информации — получение данных из открытых источников, нет прямого взаимодействия с системой, действия очень трудно обнаружить.
- Активный сбор информации — получение данных от целевой системы, все действия могут быть обнаружены, администраторы могут принять меры для пресечения дальнейших действий.
- Доступ к системе идет по средствам эксплуатации найденных уязвимостей.
- Закрепление в системе необходимо для того, чтобы продолжить атаку, не прибегая к повторному взлому.
- Скрытие следов пребывания поможет остаться незамеченными и продолжить проведение аудита.