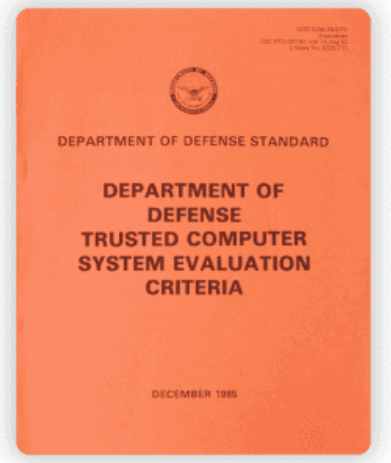
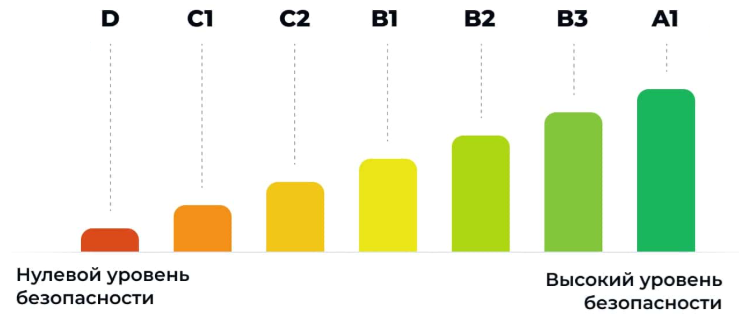
**Лекция 11**

**Классы безопасности информационных систем. Иностранные стандарты мониторинга ИБ.**

В основу большинства известных классификаций безопасности информационных систем легла система, предложенная в 1983 в документе «*Критерии определения безопасности компьютерных систем*», выпущенным Минобороны США. Этот документ также называется «Оранжевой книгой».



В «Оранжевой книге» описаны 4 уровня ИБ (D, C, B, A), разделенные на классы от самого низкого к высокому: C1, C2, B1, B2, B3, A1:



Таким образом, классов ИБ всего шесть. Разберем их подробнее.

**Уровень D** назначается ИС, безопасность которых была оценена, при этом была признана неудовлетворительной.

**Уровень C — Дискреционная защита –** пользователи могут получить допуск только к тем данным, на которые им предоставлено разрешение.

**Уровень B — Мандатная защита.** Подразумевает принудительное управление доступом на основе классификации информации и допуска пользователя. Основными требованиями этого уровня являются использование меток безопасности (пользователя или ресурса), а также создание и внедрение формальной или неформальной политики безопасности.

**Уровень A — Верифицируемая безопасность.** Уровень A представлен классом A1, в нем, дополнительно к требованиям класса B3, необходимо: протестировать систему на устойчивость к внедрению и утечкам информации; управлять настройками на протяжении всех стадий жизненного цикла ИС; создать документы, подтверждающие соответствие архитектуры информационной системы уровню безопасности A.

**Стандарт оценки безопасности информационной системы ISSAF**

Стандарт ISSAF (Information System Security Assessment Framework) разрабатывается и поддерживается группой безопасности открытых информационных систем OISSG (Open Information Systems Security Group).

Стандарт ISSAF представляет собой постоянно рецензируемый документ, содержащий информацию о том, как проводить тесты на проникновение. Сильной стороной ISSAF является показ связи между различными задачами проекта и инструментами для их достижения. Несмотря на то, что разработчики не отдают предпочтения тому или иному программному обеспечению, в своей работе вы так или иначе будете использовать большую часть предложенного ими. Стандарт предусматривает несколько фаз оценки ИБ.

**Первая фаза — планирование и подготовка**

В этой части описываются шаги, которые необходимо сделать перед началом работ: обмен вводными данными, планирование ресурсов и подготовка. В первую очередь вам необходимо заключить договор о выполнении работ, он должен быть подписан обеими сторонами. Данное соглашение будет являться основой для проведения дальнейших работ. Также вам необходимо спланировать даты, время проведения тестов, технические детали и другие необходимые условия. Этот этап, помимо прочего, включает в себя уточнение списка контактных персон с обеих сторон, организацию собрания для обсуждения необходимых деталей проведения будущих работ, согласование ранее намеченного плана.

**Вторая фаза — аудит ИС**

Вторая фаза в ISSAF проработана достаточно подробно, в ней описываются шаги, которые необходимо сделать для качественного проведения аудита. Одной из сильных ее сторон является уровень детализации. Тут представлены не только сами инструменты для выполнения тестов, но и примеры их использования. Даже если вы не знакомы со спецификой ИБ-аудита, в некоторых случаях вы сможете провести вполне удачную серию тестов, используя только приведенные примеры.

Помимо описания самих программ, примеров их запуска и использования, в ISSAF также трактуются полученные результаты, что, несомненно, расширит ваши знания даже после простого прочтения. Это не самый лучший вариант проведения аудита, но для тех, кто только знакомится с областью ИБ, он вполне подойдет.

Обратите внимание на то, что в данном фреймворке до конца не раскрывается весь потенциал тех или иных инструментов. Также здесь не описаны все возможные интерпретации полученных данных — это и понятно, ведь их очень много, да и авторы не преследовали такой цели.

В представленном ISSAF фреймворке каждый этап описывается как слой, ниже приводится краткое описание каждого из них:

– сбор информации (использование интернета для поиска всей доступной информации о цели с помощью как технических, так и нетехнических методов);

– картирование сети (идентификация всех систем и ресурсов целевой ИС);

– идентификация уязвимости (действия, выполняемые специалистом для обнаружения уязвимостей в целевой ИС);

– проникновение (получение несанкционированного доступа путем обхода методов защиты и попытка получения как можно более высоких привилегий в системе);

– получение доступа и повышение привилегий (попытка получить более высокие привилегии после успешного взлома системы или сети экспертом);

– продолжение проникновения (получение дополнительной информации о процессах в подконтрольной системе с целью ее дальнейшего использования);

– компрометация удаленных пользователей/сайтов (использование доверительных отношений и связей между удаленными пользователями и системами предприятия);

– поддержание доступа (использование скрытых каналов и руткитов для сокрытия присутствия специалиста в системе или обеспечения постоянного доступа к скомпрометированному ресурсу);

– сокрытие следов (устранение всех признаков взлома путем скрытия файлов, очистки журналов, обхода проверок целостности и антивирусного ПО).

Указанные этапы взлома применяются по отношению к следующим типам ресурсов: сети, хосты, приложения, базы данных.

В ISSAF есть разделы ИБ по нескольким направлениям:

**– Сетевая безопасность.** ISSAF с различной степенью детализации предоставляет подробную инфор­мацию о различных типах оценки безопасности сетевых устройств. Во фрейм­ворке представлена справочная информация по различным темам, примеры стандартных конфигураций, список используемых средств для проведения атак и ожидаемые результаты. Указанная информация будет интересна не только новичкам, но и специалистам с опытом работы в сфере ИБ. Ниже приведены некоторые темы, освещаемые данным фреймворком:

– взлом паролей;

– оценка безопасности коммутатора;

– оценка безопасности маршрутизатора;

– оценка безопасности файервола;

– оценка безопасности системы обнаружения вторжений (IDS);

– оценка безопасности виртуальной частной сети (VPN);

– оценка безопасности антивирусной системы;

– безопасность сети хранения данных (SAN);

– оценка безопасности беспроводной локальной сети;

– безопасность пользователей интернета.

**– Безопасность хостов –** описаны вопросы безопасности самых популярных операционных систем, среди которых Unix/Linux, Windows, Novell Netware. Предоставлена и информация о веб-серверах.

**– Безопасность приложений.** На самом деле разделить тестирование приложений и баз данных достаточно сложно. В наши дни многие приложения активно используют базы данных того или иного типа, так что, получая к ним доступ, вы получаете и доступ к базе данных. В рамках фреймворка рассматриваются следующие типы атак: атаки на веб-приложения, SQL-инъекции, аудит исходного кода, аудит бинарных файлов.

– **Безопасность баз данных –** описаны специфические методы, применимые именно к базам данных: удаленный взлом баз данных, манипуляция процессами, полный аудит баз данных.

– **Социальная инженерия.**

**Третья фаза — отчетность, избавление от следов пребывания.**

В данном разделе описаны необходимые шаги, которые следует выполнить по завершении аудита ИС. Они включают подготовку и передачу данных лицам, указанным на первом шаге, а также вопросы конфиденциальности полученных данных.

Отчет

Данный фреймворк описывает два вида отчетов — устный и письменный. Первый стоит использовать в случае нахождения критической уязвимости, которая, на ваш взгляд, должна быть устранена немедленно. Информацию о таких случаях также необходимо внести в финальную версию письменного отчета.

По мнению разработчиков, финальный отчет должен содержать следующую информацию:

– данные об организационных мероприятиях;

– цели проведения работ;

– используемое ПО;

– используемые эксплойты;

– даты и время тестов;

– все полученные данные;

– список найденных уязвимостей;

– рекомендации по устранению найденных уязвимостей, ранжированные в порядке приоритетности.

Финальный отчет не рекомендуется перегружать огромным количеством данных – не включайте все в основной документ, вынесите что-то в приложение. Так вы предоставите всю необходимую информацию, а результат вашей работы будет выглядеть намного лучше.