**Лекция 1. Основные направления практической информационной безопасности**

Информационная безопасность сегодня приобретает очень огромную роль во всей нашей жизни. Если раньше она была разбросана по разным другим областям, например, военное дело или математика, то сейчас она представляет собой целостную область.

Однако нельзя назвать её наукой, особенно ту часть, которую мы будет рассматривать. В центре нашего внимания будет именно практическая информационная безопасность.

Стоит отметить что мы частично коснёмся вопросом так называемой бумажной ИБ, но это будет лишь частично и в виде рассмотрения основных законов и правонарушений в ИБ.

Практическая каждая из областей практической ИБ связана с программированием, поэтому нужно знать и понимать основы программирования, а также ОС, сетей, информатики и математики.

Однако необязательно быть отличным математиком или информатикой, нужны лишь базовые понятия и аспекты этих больших областей.

Итак, давайте разберёмся какие основные области у нас есть:

1) Анализ уязвимостей веб приложений.

2) Анализ уязвимостей криптосистем и алгоритмов.

3) Анализ уязвимостей ОС.

4) Анализ уязвимостей десктопных приложений.

5) Анализ уязвимостей встраиваемого ПО.

6) Пентест

7) Расследование кибер преступлений

Пожалуй, на сегодня данные направление - основные, по которым можно найти хорошо оплачиваемую и интересную работу. Есть много других мелких подкатегорий над данными, но их мы рассмотрим на следующих лекциях.

Вы можете обратить внимание, на то, что большая часть направлений связана с поиском уязвимостей. В чём же заключаются уязвимости, чаще всего в 99% случаев это некие ошибки, которые были допущены при разработки определённого ПО, продукта, ОС итд.

То есть мы фактически должны найти ошибки людей, разрабатывавших данную систему. Пентест же, это полноценный анализ сети какой-либо компании, предприятия.

Пентест требует от людей высокого уровня навыков в различных сферах, таких как сети, ОС, анализ веб-приложений, а также высокого уровня общих знаний об публичных уязвимостях.

Думаю, с расследованием кибер преступлений всё приблизительно понятно. Данный вид деятельности обычно проводиться ФСБ и МВД при поддержке ряда ИБ компаний.

Теперь давайте разберёмся в каждом направление чуть подробнее.

**1. Анализ уязвимостей веб приложений.**

Одна из самых крупных отраслей практической ИБ — это анализ веб приложений. Под данным термином понимаются различные виды анализа.

Вообще существует три базовых метода анализа любой системы:

1) Белый ящик - White Box (нам даны все исходные данные системы, сама система, мы можем полностью отследить какой путь проходят наши входные данные)

2) Серый ящик - Grey Box (нам даны не все исходные данные системы, а лишь их небольшая часть, также мы имеем системы, но полностью отследить путь наших данных мы не можем)

3) Чёрный ящик - Black Box (нам дана лишь системы, которая получает от нас данные и выдаёт нам уже обработанные данные, ничего кроме этого мы не знаем и нам не дано)

Конечно самый сложный анализ — это чёрный ящик, однако он и самый приближенный к реальности, ибо если на ваше веб-приложение захотят устроить атаку, то поиск уязвимостей и разработка векторов будет происходить по методу чёрного ящика.

Однако довольно часто компании заказывают анализ по типу белого ящика, и предоставляют все исходные коды, тем самым они также имеют шанс на усовершенствование их кода, который может быть и не связан с ИБ частью их веб приложения.

Основные уязвимости в вебе уже давно не меняются, однако новые виды атак появляются с завидно регулярностью, но всё же базовые уязвимости, которые были действенные 10 лет назад сейчас находятся также на 1 месте по частоте встречаемости.

OWASP TOP 10:

* 1. Injection – инъекции различного типа.
  2. Broken Authentication and Session Management
  3. Cross-Site Scripting (XSS)
  4. Broken Access Control
  5. Security Misconfiguration
  6. Sensitive Data Exposure
  7. Insufficient Attack Protection (NEW)
  8. Cross-Site Request Forgery (CSRF)
  9. Using Components with Known Vulnerabilities
  10. Underprotected APIs

Наверное, это базовые уязвимости и атаки, которые встречаются в веб приложениях.

Также есть множество разнообразных уязвимостей по типу ошибок логики, или слабых паролей, неправильно настроенных прав на просмотр директорий, заливки шелла, но это больше ляпы, чем атаки и уязвимости.

**2. Анализ уязвимостей криптосистем и алгоритмов.**

Очень узко направленная область, которая очень часто используется спец. службами или математиками-криптографами, которые пытаются ломать алгоритмы математически.

Если рассматривать практику в плане хакерских атак, то тут всё довольно тривиально, иногда при Пентест может потребоваться умение анализировать безопасность криптосистем, то есть должно быть выработано понимание какую системы можно взломать, а какую нет.

Большинство уязвимостей здесь связано с неправильными параметрами системы, например, слишком маленькая секретная экспонента RSA, либо маленькие ключи AES, так-же стоит отметить использование старых алгоритмов шифрования, которые раньше возможно и были эффективны, но сегодняшние мощности компьютеров ломают данные системы за пару минут.

Вообще стоит отметить что всё что связано с криптографией в России контролируется ФСБ, поэтому здесь всё очень узко и понятно.

**3. Анализ уязвимостей ОС.**

При рассмотрение данной тематики стоит понимать, что в этой области атаки чаще всего идут на ядро операционной системы.

Вектора бывают различны, и в отличии от веб-уязвимостей здесь всё гораздо сложнее.

Стоит также отметить, что ОС бывают разные, десктопные, консольные, встраиваемые, свободно распространяемые или коммерчески, в зависимости от этих параметров безопасность будет разная.

Основные моменты, которые будут интересовать исследователей во время поиска уязвимостей - это удалённые атаки, то есть атаки с помощью уязвимостей в сетевых сервисах.

Через такой тип атак можно распространять зловредное ПО, начиная от шпионского и заканчивая криптолокерами. К слову благодаря уязвимости в SMB был распространён вымогатель Wanacry и NotPetya

Также есть и локальные атаки на ОС, например, повышение привилегий прямо на машине, или обход каких-либо механизмов, ограничивающих ваши действия, например, UAC в Windwos.

Примерно те же уязвимости ищутся и в встраиваемых ОС, однако там всё гораздо сложнее, ибо зачастую закрепиться на машине не удаётся, также не удаётся отлаживать сервисы, и в целом исследования проходят гораздо дольше и сложнее.

Встраиваемое ПО чаще всего используется в системах управления каких-либо процессов, будь то умный чайник, автомобиль, дом, терминал оплаты, или контроллер, на АЭС который регулирует скорость вращения центрифуги.

**4. Анализ уязвимостей десктопных приложений.**

Практически идентичная область, что и ОС по типу уязвимостей и по видам исследования, однако здесь мы разбираем само приложение, а оно чаще всего имеют другую принципиальную схему работы и логики.

Конечно анализируются не все подряд приложения, а те которые очень часто используются людьми или компаниями.

Например, движки веб-серверов, крипто-библиотеки, разнообразные текстовые читалки и редакторы итд.

Также в этой сфере отдельным особняком стоит вирусная аналитики и вирусология. Но это очень большая отдельная тема.

**5. Анализ уязвимостей встраиваемого ПО.**

Итак, данная тема уже была рассмотрена. однако стоит затронуть её чуть подробнее.

Дело в том, что эта область довольно малоизвестна широкому кругу лиц, но несмотря на мелкую огласку она одна из самых критичных.

В чём же заключается проблема, как было сказано вскользь в теме про анализ уязвимостей ОС, встраиваемые ОС чаще всего используются для управления какими-либо системами без вмешательства человека.

То есть во всей автоматике которая нас с вами окружает присутствуют прошивки, которые зачастую являются встраиваемыми ОС реального времени.

Критически объекты инфраструктур управляются с помощью контроллеров на которых установлены встраиваемые ОС, и если скомпрометировать один из таких контроллеров то последствия могут быть очень критичны.

**6. Пентест**

Пентест - по сути является полноценным анализом сети компании на возможные векторы проникновения и компрометации.

На деле же является одой из самых популярных услуг, которые заказывают у ИБ компаний.

Обычно пентест проводят не один, не даже группа специалистов в области безопасности веб приложений, чаще всего пентест проводит несколько различных групп специалистов в той или иной области.

Нельзя относится к пентесту как к ломанию только веб-сервера и нахождения SQLi или RCE.

Настоящий пентест проводится довольно основательно, начиная с базового сбора информации и заканчивая правильным закреплением в сети и сливом все возможной информации из компании, при этом желательно ни оставить никаких следов.

Грамотно проведённый пентест позволяет компании иметь практически 100% защиту от будущих атак, исключая уязвимости нулевого дня.

**7. Расследование кибер преступлений**

Теперь перейдём к пункту, который может начаться если вы что-то вдруг решили поломать и не следили за своей анонимностью.

Итак, всё что касается расследования преступлений проводится МВД, ФСБ и специальным отделом К в ФСБ, чаще всего при помощи крупных компаний, на которых были проведены атаки, или просто кампаний-помощников в расследование, например, национально-ориентированных атак.

В России, например, часто МВД и ФСБ сотрудничают с Лабораторией Касперского или с Group-IB для нахождения преступников.

Мы рассмотрели основные направления практической безопасности, которые сегодня популярны и актуальны и по которым можно найти интересную работу.

На следующих лекциях мы будем подробно разбирать азы каждой из сфер практической ИБ.