**Лекция 2.1. Введение в компьютерную безопасность**

В данной лекции будут рассмотрены следующие вопросы:  
1. Основы компьютерной безопасности, включая процедуру проведения атаки и базовый набор мер по обеспечению защищённости компьютерных систем.  
2. Установка и настройка необходимых инструментов в области обеспечения информационной безопасности, включая сканеры уязвимостей, анализаторы сетевого трафика, системы обнаружения вторжений.

### Глава 1. Введение в компьютерную безопасность

**Компьютерная безопасность заключается в постоянном процессе обеспечения конфиденциальности, целостности и доступности информации.**  
Слово «процесс» выделено не зря: казалось бы, давайте настроим безопасную систему, так, чтобы подобраться к защищаемой информации было невозможно, закроем все лазейки, напишем строгие правила фильтрации трафика. Но, к сожалению, это невозможно. Постоянное развитие методов атак на компьютерные сети заставляет постоянно модернизировать и средства защиты, закрывать уязвимости. Следовательно, изучение методов обеспечения информационной безопасности становится необходимостью для любого человека, работающего в сфере IT.  
Для того, чтобы проникнуть в защищённую сеть, злоумышленнику в ряде случаев требуется найти в этой сети уязвимость. Уязвимостью могут быть ошибки в настройке сетевого оборудования, устаревшие базы антивирусных программ. Даже пользователь, открывающий ссылки из писем с обещанием выигрыша в лотерее, в какой-то степени тоже является уязвимостью.  
Уязвимость — слабое звено в информационной системе. Как правило, уязвимости позволяют получить несанкционированный доступ к информации, получить управление над операционной системой или отдельными её компонентами, либо вызвать отказ в обслуживании. Какие-то уязвимости настолько сложны для эксплуатации и практически не дают злоумышленнику никаких привилегий, поэтому такие уязвимости относят к некритичным. Определённые уязвимости эксплуатируются по щелчку пальцев, а эффект — гигантский. Такие уязвимости, само собой, стоит относить к критическим.  
Уязвимости делятся на:  
1. Известные уязвимости. Имеют свой CVE либо информация о них была выложена в публичный доступ.  
2. Неизвестные уязвимости. Неизвестные уязвимости просто существуют, а знает о них либо никто, либо очень ограниченный круг людей. Неизвестные уязвимости также называют 0-day (zero day) или «уязвимость нулевого дня».  
Для устранения уязвимостей в программных продуктах производители ПО регулярно выпускают исправления, называемые патчами.  
**Поиск уязвимостей** — важная часть задачи обеспечения безопасности. Для этого необходимо регулярное тестирование системы. Часто процесс тестирования автоматизируется при помощи автоматических сканеров уязвимостей (которые нередко применяются и злоумышленниками). Однако, автоматическое тестирование не всегда может показать все проблемы в безопасности системы. Поэтому для поиска уязвимостей периодически стоит проводить тестирование на проникновение (пентест) — моделирование действий злоумышленников с целью оценки безопасности системы. Наличие уязвимости представляет собой угрозу того, что этой уязвимостью может кто-то воспользоваться в злонамеренных целях.

### Глава 2. Введение в компьютерную безопасность

Угроза — набор обстоятельств и действий, которые могут привести к нарушению безопасности системы.  
Любую угрозу можно условно описать тремя характеристиками:  
1. Субъект (источник) угрозы (например, злоумышленник).  
2.  Объект угрозы (к примеру, база данных на сервере).  
3.  Реализация угрозы (получение злоумышленником несанкционированного доступа к базе данных).  
Атака — реализованная угроза. Успешно реализованная атака приводит к возникновению ущерба:  
Приведем пример: В программном коде OS Windows обнаружена новая уязвимость CVE-2021-12345 (таким кодом обозначаются все уязвимости в базе ссылка [https://cve.mitre.org](https://cve.mitre.org/)). Появление информации об этой уязвимости в общем доступе порождает угрозу. Реализация этой угрозы — атака с использованием эксплойта для данной уязвимости.  
Стоит также добавить, что угрозы можно разделить на внешние и внутренние, умышленные и непреднамеренные.  
Разберёмся в них на примерах:  
1. Сканирование портов веб-сервера, доступного из сети Интернет можно отнести к внешней умышленной угрозе.  
2. Ошибка в конфигурации сетевого оборудования, которая привела к потере доступа в Интернет — внутренняя непреднамеренная угроза.  
3. А вот сканирование локальной сети организации с хоста из этой сети можно уже отнести к внутренней умышленной угрозе.  
Важной задачей обеспечения информационной безопасности является управление рисками. Риск — оценка ущерба от атаки с учётом вероятности её реализации.  
Управление рисками представляет из себя постоянный анализ угроз, прогнозирование и оценку возможных последствий их реализации для организации, распределение угроз по степени их возможного осуществления, опасности их последствий. Завершаться данный процесс должен принятием решения о выборе мер по предотвращению или смягчению последствий от реализации той или иной угрозы, иначе говоря, всё сводится к минимизации риска.

Шаги кибератаки:

1. **Разведка.** Всё начинается с того, что злоумышленник выбирает компанию-жертву. Эту стадию атаки невозможно отследить и проконтролировать. Хакер проводит исследование, чтобы выяснить, насколько велик куш, а также во сколько ему обойдется атака
2. **Выбор оружия.** На следующем этапе преступник занимается разработкой или выбором инструментов для атаки.
3. **Доставка.** На третьем этапе зловред доставляется в сеть организации. Это чаще всего происходит через зараженные письма, которые открывают сами сотрудники.
4. **Взлом.** Пользователь открывает письмо (или скачивает файл), открывает документ, тем самым активируя вредоносную программу, и злоумышленник получает контроль над зараженной машиной. Его цель на этом этапе — избежать обнаружения и скачать оставшиеся модули
5. **Установка и развертывание зловреда.** Компьютер уже находится под контролем хакера, который копирует другие модули, создает постоянное присутствие.
6. **Полный контроль и управление**. Зараженные машины под полным контролем хакера: злоумышленник может отправлять команды, присылать новые модули для атаки. Он получает информацию о том, что это за компьютер, какое ПО на нем установлено
7. **Ущерб**. На финальном этапе хакер переходит к достижению своих целей — начинает шантажировать пользователя, скачивает нужные ему данные, переводит деньги.
8. **Набор процедур и инструментов, которые обеспечивают всестороннюю защиту конфиденциальной информации от неправильного использования, несанкционированного доступа, искажения или уничтожения — это:**
   1. Угроза безопасности
   2. Уязвимость
   3. ИБ
   4. Ценность информации
9. **Выберите ВСЕ этапы процедуры атаки:**
   1. Подбор инструментов
   2. Шантажирование
   3. Разведка
   4. Управление и полный контроль
   5. Доставка
10. **Сканирование портов веб-сервера, доступного из сети Интернет — это:**
    1. Внешняя угроза
    2. Все ответы верны
    3. Внутренняя угроза
11. **На каком этапе процедуры атаки хакер переходит к достижению своих целей: начинает шантажировать пользователя, скачивает нужные ему данные, переводит деньги?**
    1. Установка и развертывание
    2. Выбор инструментов
    3. Ущерб
    4. Полный контроль и управление
    5. Разведка
    6. Взлом
    7. Доставка
12. **Оценка ущерба от атаки с учётом вероятности её реализации — это:**
    1. Риск
    2. ИБ
    3. Установка и развертывание
    4. Ценность информации
    5. Управление рисками
13. **На каком этапе процедуры атаки происходит рассылка заражённых писем, которые открывают сами сотрудники?**
    1. Установка и развертывание
    2. Взлом
    3. Разведка
    4. Доставка
    5. Выбор инструментов
    6. Полный контроль и управление
    7. Ущерб
14. **Ошибка в конфигурации сетевого оборудования, которая привела к потере доступа в Интернет:**
    1. Внешняя угроза
    2. Все ответы верны
    3. Внутренняя угроза
15. **Постоянный анализ угроз, прогнозирование и оценку возможных последствий их реализации для организации, распределение угроз по степени их возможного осуществления, опасности их последствий — это:**
    1. Управление рисками
    2. Ценность информации
    3. Риск
    4. ИБ
    5. Установка и развертывание
16. **На каком этапе атаки пользователь открывает письмо (или скачивает файл), открывает документ, тем самым активируя вредоносную программу?**
    1. Выбор инструментов
    2. Взлом
    3. Доставка
    4. Полный контроль и управление
    5. Ущерб
    6. Установка и развертывание
    7. Разведка
17. **Если уязвимости настолько сложны для эксплуатации, что практически не дают злоумышленнику никаких привилегий, то эти уязвимости относят к:**
    1. Критическим уязвимостям
    2. Некритичным уязвимостям