ВВЕДЕНИЕ В КИБЕРБЕЗ

01. Введение

Немного обо мне

Студент Университета Иннополис, 3 курс

CTF enjoyer. Во многих был финалистом

Навыки: python, networks, web pentest

Pentester @ FearsOff ☺

← Ищите меня здесь

Правила работы

- Мы на «Ты»
- Время работы: 9:00 - 12:00, 14:00 – 16:00
- Райтапы **не читаем**
- Если **что-то** непонятно – спрашивайте. Я не кусаюсь
- Можете писать мне в личку с 12:00 до 20:00
- Так же QR нашего чатика:

Для работы необходимо:

- Ноутбук
- Windows/UNIX
- Если Windows, то придется поставить VirtualBox с Kali Linux

Что такое информация?

Что такое информация?

Сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств).

Знания относительно фактов, событий, вещей, идей и понятий, которые в определённом контексте имеют конкретный смысл

Что такое безопасность?

Безопасность - состояние защищённости жизненно важных интересов личности, общества, государства от внутренних и внешних угроз

Безопасность - состояние, при котором отсутствует опасность

Безопасность являет собой защиту интересов субъектов информационных отношений.

Классификация “безопасностей”

- *Личная*
- *Государственная*
- *Пожарная*
- *Пищевая*
- *Экологическая*
- ***Информационная***

Классификация “безопасностей”

- *Личная*
- *Государственная*
- *Пожарная*
- *Пищевая*
- *Экологическая*
- ***Информационная***

Тогда что такое Информационная безопасность?

Информационная безопасность

ИБ – состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере

ИБ – это процесс обеспечения конфиденциальности, целостности и доступности информации.

Безопасность информации – состояние защищенности данных, при котором обеспечиваются их конфиденциальность, доступность и целостность

А что такое кибербезопасность?

Кибербезопасность

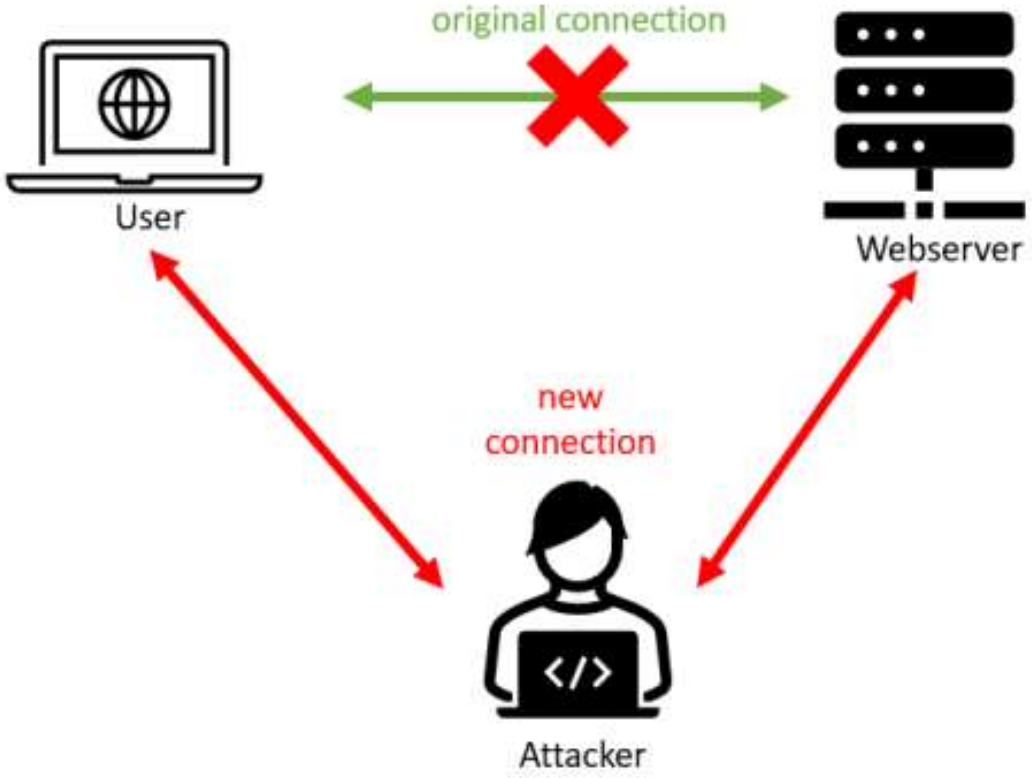
КБ – это совокупность
методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

«Три кита» информационной безопасности

- *Доступность*
- *Целостность*
- *Конфиденциальность*

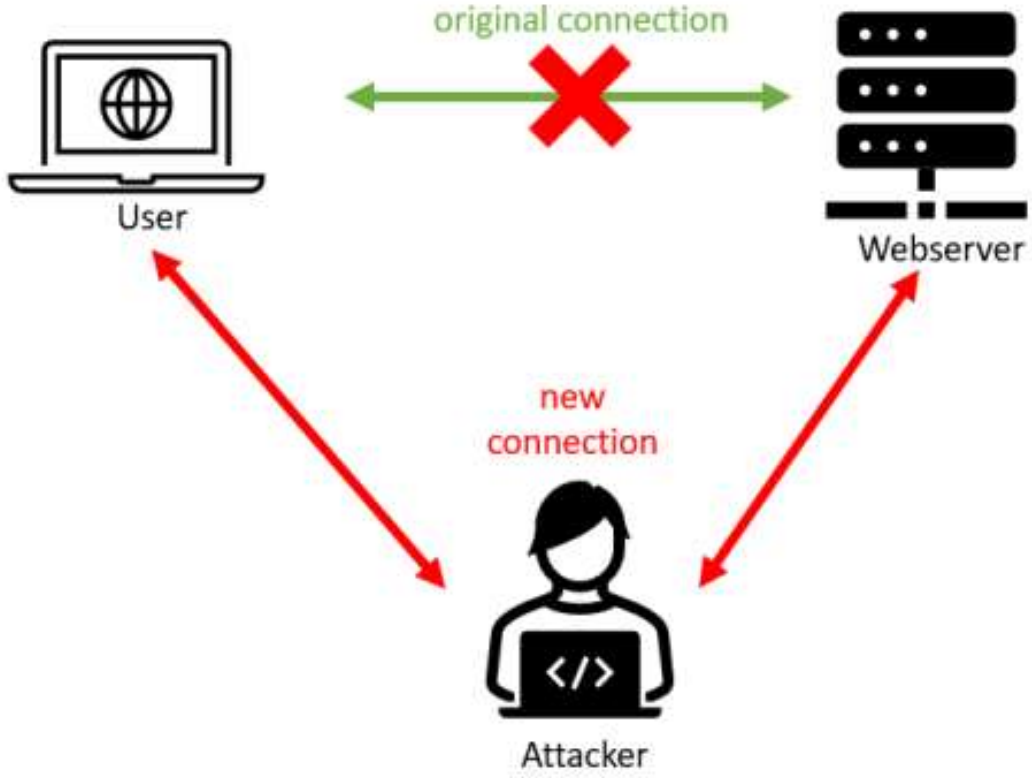
Конфиденциальность

MiM не может прочитать информацию переданную User



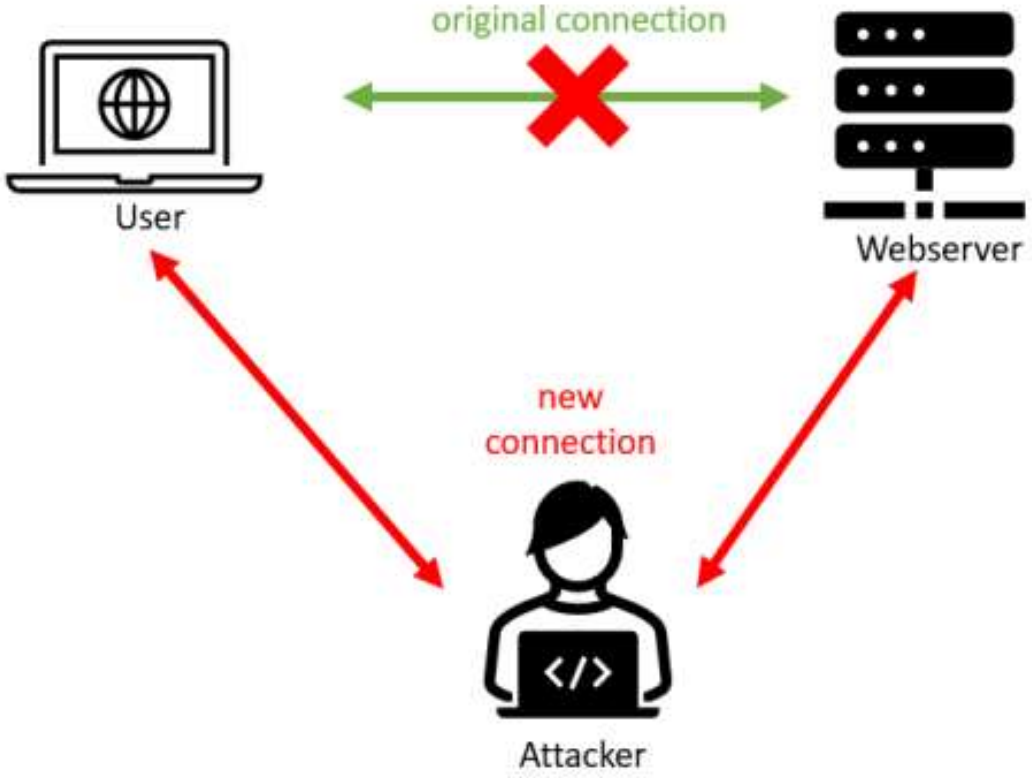
Целостность

Информация, переданная User, не была изменена несанкционированным образом



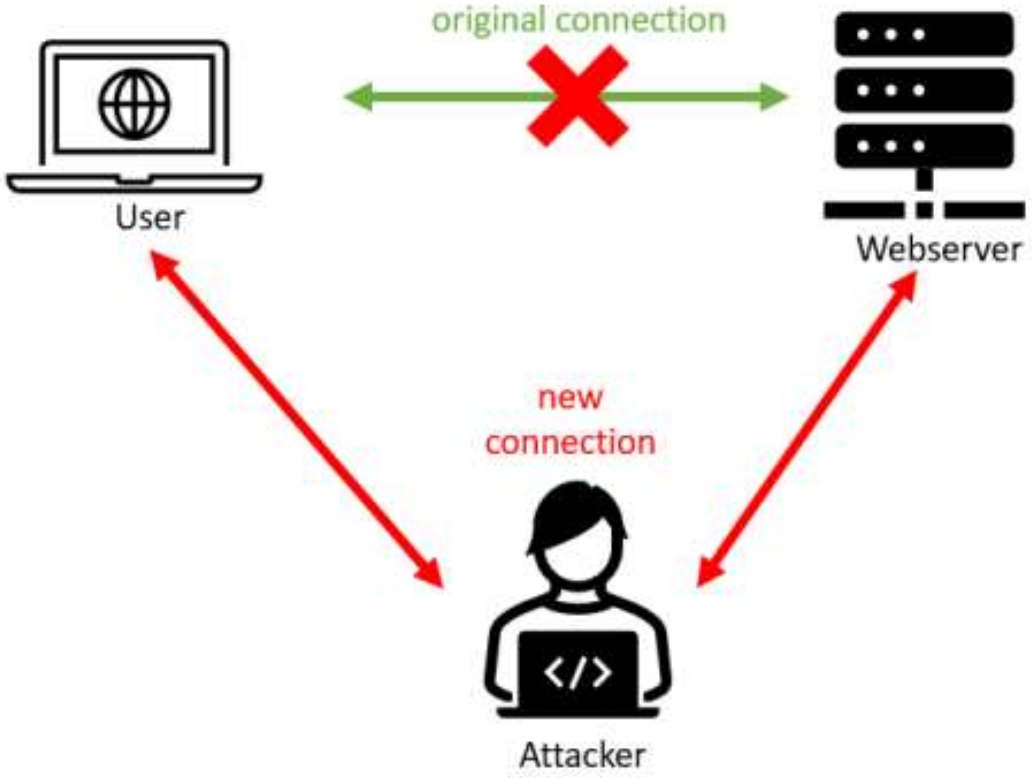
Неотказуемость

После того как User купил что-то и потратил деньги, он не может заявить банку, что деньги он не тратил



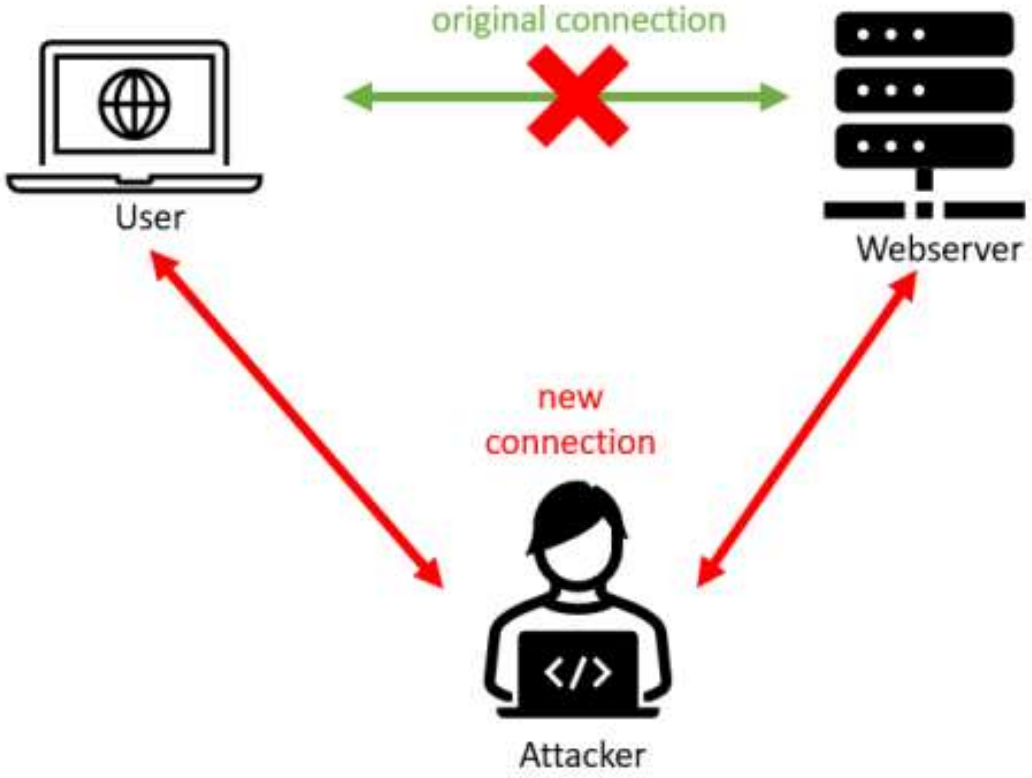
Авторизация

User не может зайти в админ панель, если он не админ. Не путать с **аутентификацией**



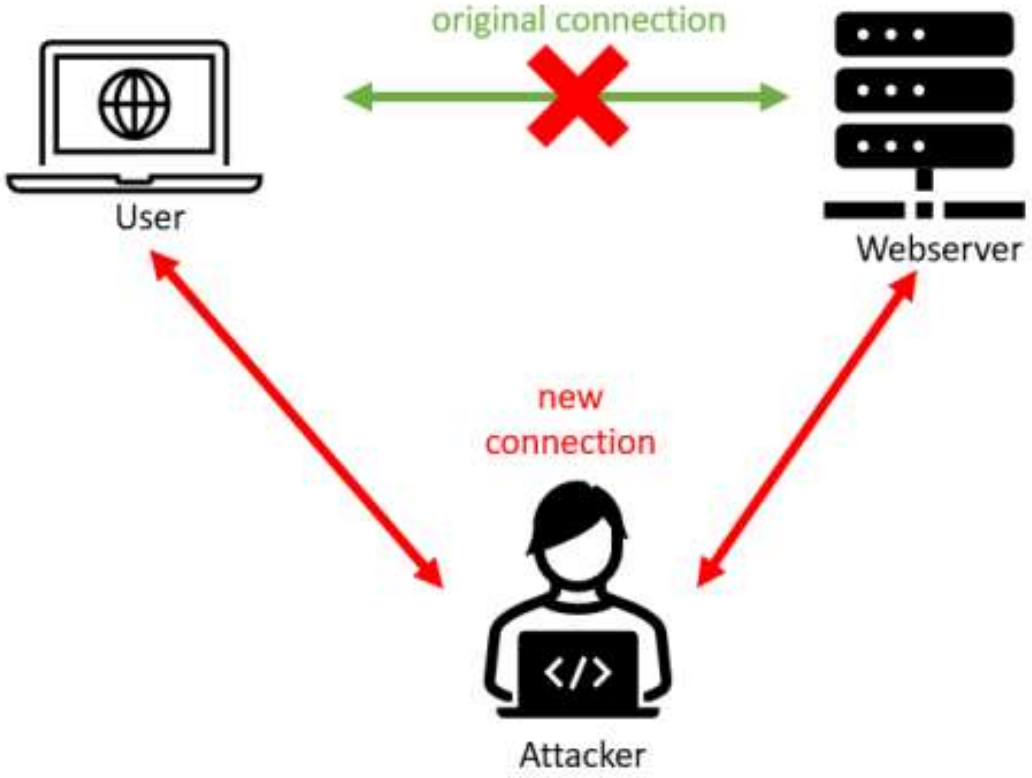
Надежность

User не может зайти в админ панель, если он не админ. Не путать с **аутентификацией**



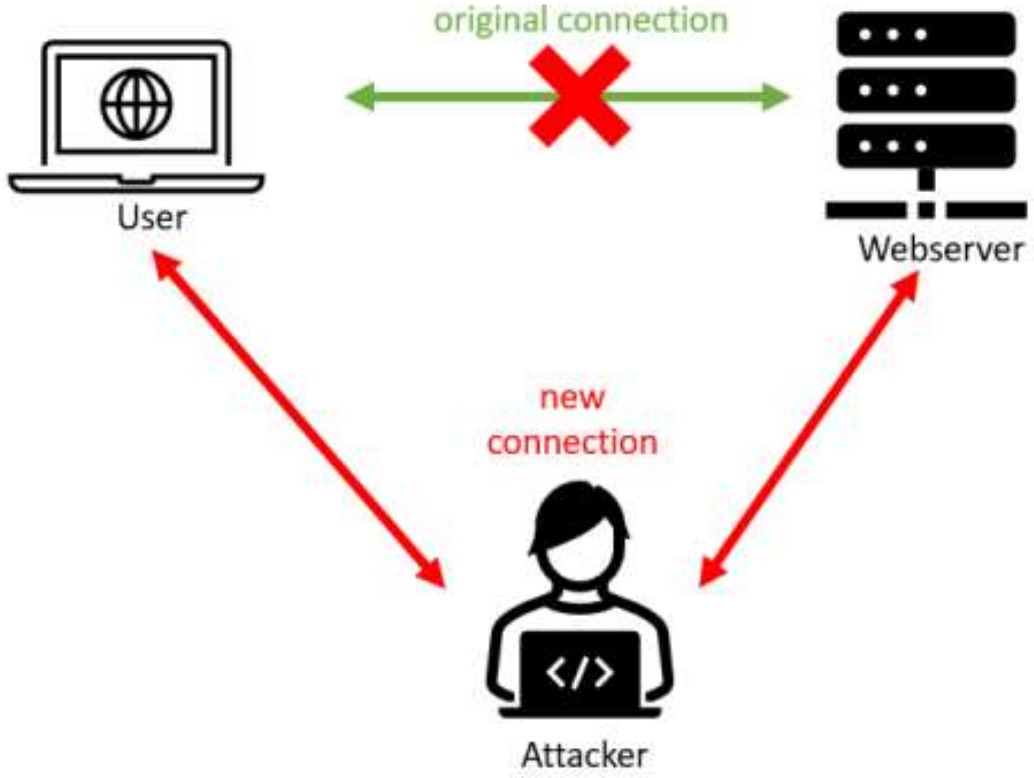
Доступность

Информация доступна и может быть изменена своевременно и с доступными в данный момент правами. MiM не может прервать соединение User и Webserver



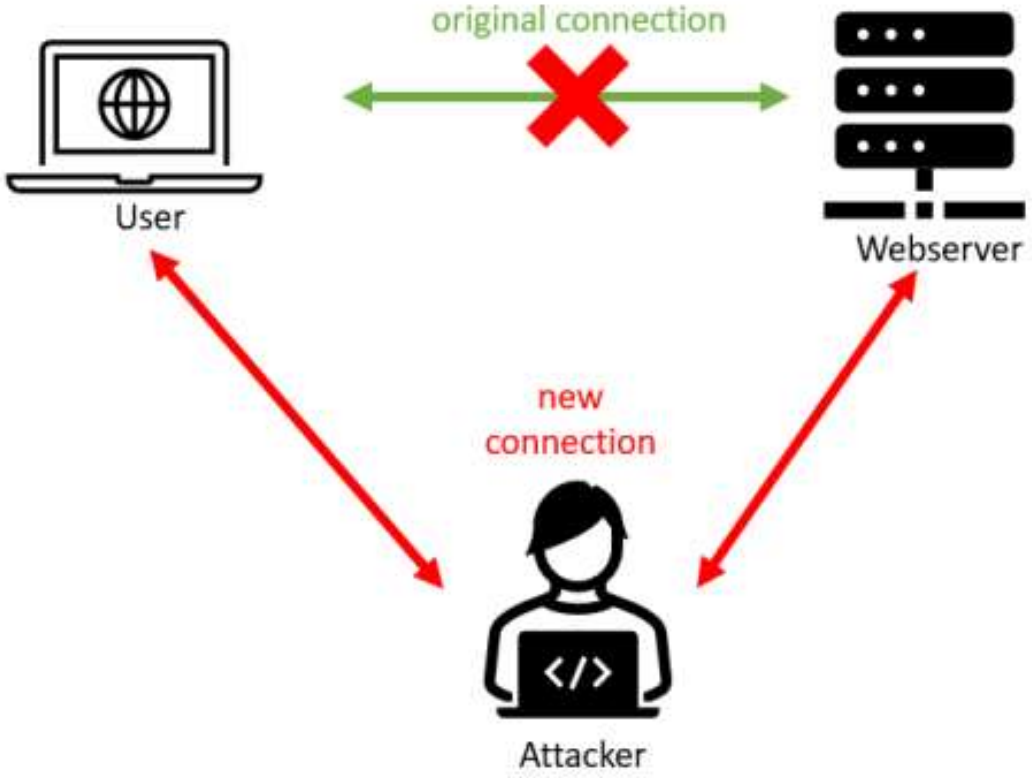
Аутентификация

Соотношение лично
сти/роли. Это определение
может быть выполнено
несколькими различными
способами, но обычно оно
основано на комбинации
Например:



Аутентификация

Соотношение лично
сти/роли. Это определение
может быть выполнено
несколькими различными
способами, но обычно оно
основано на комбинации
Например:
- Пароль + 2FA



Средства защиты целостности

Средства защиты целостности

КБ – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

Шифрование

Преобразование информации с использованием секретного ключа, называемого ключом шифрования, так что преобразованная информация может быть прочитана только с помощью другого секретного ключа, называемого ключом дешифрования (который в некоторых случаях может быть таким же, как ключ шифрования)

Контроль доступа

Правила и **политики**, которые ограничивают доступ к конфиденциальной информации этим людям и / или системам, которые не должны иметь туда доступ. Необходимость знать может определяться по пользователю, например, именем человека или серийным номером компьютера, а также роль, которую имеет человек, например, является менеджером или специалистом по компьютерной безопасности.

Средства защиты конфиденциальности

Определение того, **разрешен ли** человеку или системе доступ к ресурсам на основе политики контроля доступа. Методы авторизации должны препятствовать злоумышленнику обманывать систему, когда он может получить доступ к защищенным ресурсам.

Физическая безопасность – установление физических барьеров для ограничения доступа к защищенным вычислительным ресурсам. Такие барьеры включают в себя блокировки на шкафах и дверях, размещение компьютеров в помещениях без окон,

Средства защиты доступности

Физическая защита – инфраструктура, предназначенная для обеспечения доступности информации даже в случае физических проблем.

Резервирование – компьютеры и устройства хранения, которые служат резервами в случае сбоев

Средства защиты гарантийности

Политики – указание поведенческих ожиданий, которые люди или системы совершают. Например, разработчики онлайн музыкальной системы могут указывать политики, описывающие, как пользователи могут получать и копировать песни

Разрешения – описание поведений, разрешенное агентами, которые взаимодействуют с человеком или системой. Например, интернет-магазин музыки может предоставлять разрешения для ограниченного доступа и копирования для людей, которые приобрели определенные песни

Защита – описание механизмов, позволяющих применять разрешения и политики. Мы могли бы представить, что интернет-магазин музыки будет создавать защиту, чтобы люди не совершали несанкционированного доступа и копирования своих песен

Средства защиты аутентификации

Цифровые подписи – это криптографические вычисления, которые позволяют человеку или системе совершать аутентификацию своих документов уникальным способом, который обеспечивает **неотказуемость**

Средства защиты анонимности

Агрегация – объединение данных от многих лиц, так что раскрытые суммы или средние значения не могут быть привязаны к кому-либо

Смешивание – переплетение транзакций, информации или сообщений таким образом, который нельзя проследить никому.

Прокси – доверенные агенты, которые готовы участвовать в действиях для человека таким образом, который не может быть прослежен до этого человека.

Агент – что-то, выступающее в роли **доверенного лица, посредника,** уполномоченное совершать определенный круг действий как от своего имени, так и от имени другого лица

ИБ в России

Состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз

от 70 до 500 нормативно-правовых актов (включая акты, которыми предусматривается создание отраслевых или специализированных автоматизированных систем)

Основные законы

- Федеральный закон «Об информации, информатизации и защите информации»
- Закон «О государственной тайне»
- Федеральный закон «О связи»
- Закон «О правовой охране программ для электронных вычислительных машин и баз данных»
- Закон «Об авторском праве и смежных правах»
- **Статьи УК РФ**

Основные законы

- **272 статья УК РФ** - неправомерный доступ к компьютерной информации
- **273 статья УК РФ** - создание, использование и распространение вредоносных компьютерных программ
- **274 статья УК РФ** - нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Кто регулирует информацию?


ФСБ
ФСБ


К

РОСКОМНАДЗОР


Минцифры
России

Каких вендоров ИБ вы знаете?


positive
technologies


kaspersky


INNOSTAGE

BI.ZONE

Cybersecurity

Больше терминов

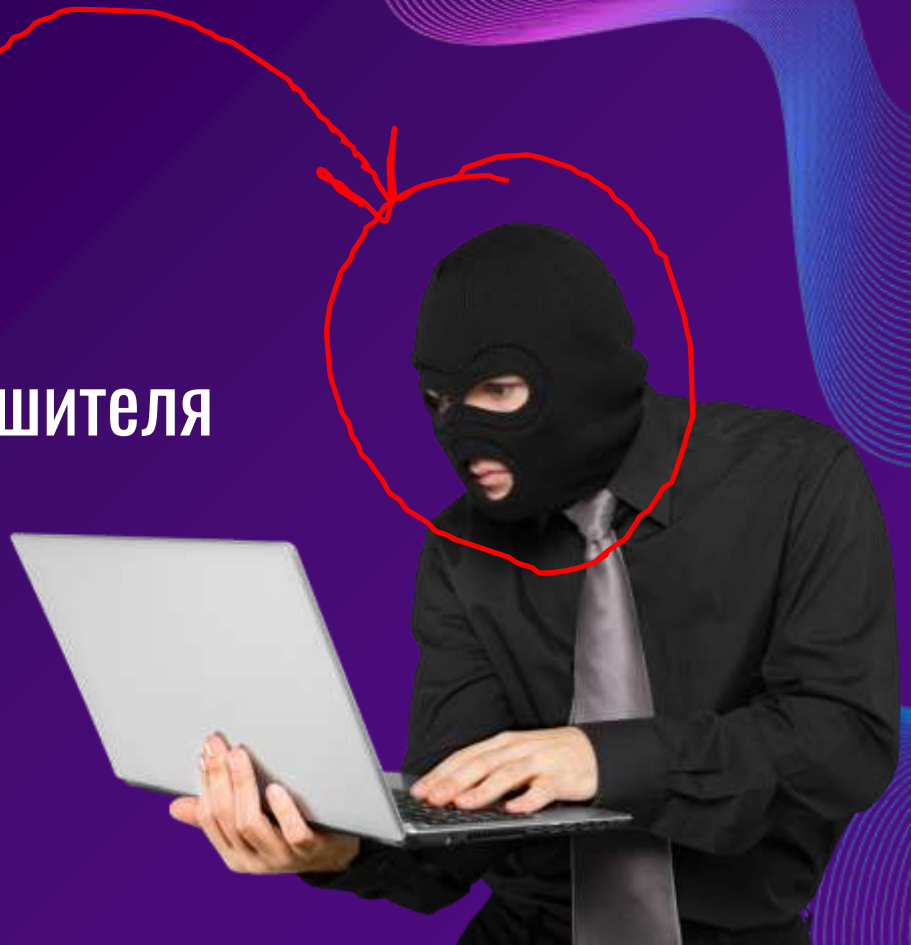
Уязвимость – слабое место в информационных системах, которым могут воспользоваться злоумышленники

Угроза – совокупность условий и факторов, создающих опасность нарушения **информационной безопасности**

Атака – воздействие на информационную систему с целью повредить её, получить или ограничить к ней доступ, собрать конфиденциальные данные.

Риск – потенциальную возможность использования уязвимостей конкретной угрозой для причинения ущерба организации. Под величиной риска условно понимают произведение вероятности негативного события и размера ущерба

Модель нарушителя



Модель нарушителя

Чтобы предотвратить действия нарушителя – нужно думать как нарушитель:

- Дана уязвимость – Z
- Дан список шагов $S_1,...S_n$ с помощью которых возможным будет эксплуатировать Z
- Мы знаем вероятность успешного выполнения каждого S
- Определены затраты на каждый шаг S

Наша задача – построить **дерево атаки**

Модель нарушителя

Чтобы предотвратить действия нарушителя – нужно думать как нарушитель:

- Дана уязвимость – Z
- Дан список шагов $S_1,...S_n$ с помощью которых возможным будет эксплуатировать Z
- Мы знаем вероятность успешного выполнения каждого S
- Определены затраты на каждый шаг S

Наша задача – построить **дерево атаки**


Взлом сейфа
Отмычка
Запомнить код
Разрезать сейф
Сменить код и открыть
Найти записку с кодом
Узнать код
Угрожать
Подслушать
Шантаж
Взятка
Наводящие вопросы
Услышать код

Модель нарушителя

Такое моделирование атак называется **деревьями атаки**

> Мы берем атаку на интересный актив как корень дерева

> Мы улучшаем эту атаку, перечисляя возможности для достижения этой атаки в качестве подузлов этого корня

> Мы рекурсивно уточняем каждый из этих подузлов, пока не получим четкое представление о порядке действия


Взлом сейфа
5000
Отмычка
25000
Запомнить код
5000
Разрезать сейф
15000
Сменить код и открыть
50000
Найти записку с кодом
9999999999
Узнать код
5000
Угрожать
10000
Подслушать
9999999999
Шантаж
10000
Взятка
10000
Наводящие вопросы
10000
Услышать код
9999999999

Модель нарушителя

Обратите внимание, что существует различие между подузлами «подслушать»!

Блоки соединены, чтобы указать тип «и»: оба базовых действия должны быть успешными!

Визуализация помогает понять тип атак, но мы также можем использовать его для количественного анализа.

Если мы добавим уровень сложности (***Низкий, Средний, Высокий, Экстремальный***) действий к блокам, можно логически вычислить итоговую сложность атаки


Взлом сейфа
средний
Отмычка
экстрим
Запомнить код
средний
Разрезать сейф
сложный
Сменить код и открыть
экстрим++
Найти записку с кодом
экстрим
Узнать код
средний
Угрожать
сложный
Подслушать
экстрим
Шантаж
сложный
Взятка
средний
Наводящие вопросы
легкий
Услышать код
экстрим

Задача:

Постройте дерево атаки для взлома компьютера своего друга ^_^

Модели угроз и атак

Подслушивание: перехват информации, предназначенной для кого-то еще во время ее передачи по каналу связи.

Маскарадинг: Изготовление информации, которая, как предполагается, принадлежит к тому, кто на самом деле не является автором.

Отказ в обслуживании: прерывание или деградация службы данных или доступа к информации.

Изменение: несанкционированное изменение информации.

Отказ: отказ в обязательстве или получение данных.

Корреляция / Traceback: интеграция нескольких источников данных и информационных потоков для определения источника конкретного потока данных или части информации.

Модели угроз и атак

Для каждой из этих угроз дайте пример и объясните, на какую **фундаментальную концепцию** они нацелены:

Подслушивание:

Модели угроз и атак

Для каждой из этих угроз дайте пример и объясните, на какую **фундаментальную концепцию** они нацелены:

Подслушивание: Wireshark, Aircrack-ng, man-in-the-middle; конфиденциальность
Маскарадинг:

Модели угроз и атак

Для каждой из этих угроз дайте пример и объясните, на какую **фундаментальную концепцию** они нацелены:

Подслушивание: Wireshark, Aircrack-ng, man-in-the-middle; конфиденциальность
Маскарадинг: фишинг, спуфинг; аутентичность, конфиденциальность
Отказ в обслуживании:

Модели угроз и атак

Для каждой из этих угроз дайте пример и объясните, на какую **фундаментальную концепцию** они нацелены:

Подслушивание: Wireshark, Aircrack-ng, man-in-the-middle; конфиденциальность
Маскарадинг: фишинг, спуфинг; аутентичность, конфиденциальность
Отказ в обслуживании: спам, атака ICMP; доступность
Изменение:

Модели угроз и атак

Для каждой из этих угроз дайте пример и объясните, на какую **фундаментальную концепцию** они нацелены:

Подслушивание: Wireshark, Aircrack-ng, man-in-the-middle; конфиденциальность
Маскарадинг: фишинг, спуфинг; аутентичность, конфиденциальность
Отказ в обслуживании: спам, атака ICMP; доступность
Изменение: Человек-в-середине; целостность
Отказ:

Модели угроз и атак

Для каждой из этих угроз дайте пример и объясните, на какую **фундаментальную концепцию** они нацелены:

Подслушивание: Wireshark, Aircrack-ng, man-in-the-middle; конфиденциальность
Маскарадинг: фишинг, спуфинг; аутентичность, конфиденциальность
Отказ в обслуживании: спам, атака ICMP; доступность
Изменение: Человек-в-середине; целостность
Отказ: захват сеанса, изменение журналов; гарантия, неотказуемость
Корреляция / Трассировка:

Модели угроз и атак

Для каждой из этих угроз дайте пример и объясните, на какую **фундаментальную концепцию** они нацелены:

Подслушивание: Wireshark, Aircrack-ng, man-in-the-middle; ***конфиденциальность***
Маскарадинг: фишинг, спуфинг; ***аутентичность***, ***конфиденциальность***
Отказ в обслуживании: спам, атака ICMP; ***доступность***
Изменение: Человек-в-середине; ***целостность***
Отказ: захват сеанса, изменение журналов; гарантия, ***неотказуемость***
Корреляция / Трассировка: отслеживание; ***анонимность***

Шкалы оценки критичности уязвимостей

CVSS

Common Vulnerability Scoring System

Attack Vector (AV): способ доступа к уязвимости (Network, Adjacent, Local, Physical).

Attack Complexity (AC): сложность атаки (Low, High).

Privileges Required (PR): уровень привилегий, необходимых для эксплуатации (None, Low, High).

User Interaction (UI): необходимость взаимодействия пользователя (None, Required).

CVSS

Scope (S): влияет ли уязвимость на другие компоненты (Unchanged, Changed).

Confidentiality Impact (C): степень влияния на конфиденциальность (None, Low, High).

Integrity Impact (I): степень влияния на целостность (None, Low, High).

Availability Impact (A): степень влияния на доступность (None, Low, High).

CVSS на примере

Задача:
Оценим критичность уязвимости на примере

> Веб-приложение имеет уязвимость **SSRF** (Server-Side Request Forgery), которая позволяет злоумышленнику отправлять произвольные HTTP-запросы от **имени сервера** имея доступ к аккаунте **модератора**. Эта уязвимость может использоваться для доступа к внутренним сервисам, базам данных и другим ресурсам, которые не должны быть доступны из внешней сети

CVSS на примере

Вектор атаки:
Сложность атаки:
Необходимые привилегии:
Необходимость действий от пользователя:
Смена скоупа:
Влияние на конфиденциальность:
Целостность:
Доступность:

CVSS на примере

Вектор атаки: сетевой
Сложность атаки: низкая
Необходимые привилегии: высокие
Необходимость действий от пользователя: нет
Смена скоупа: да
Влияние на конфиденциальность: HIGH
Целостность: LOW
Доступность: LOW

По шкале 0/10, сколько бы дали?

Го проверять:

Mitre Att&ck

Mitre Att&ck

База знаний о поведении злоумышленников, основанная на **реальных наблюдениях**. Она документирует:

1. как атакующие получают доступ к системам,
2. как они двигаются по сети,
3. какие инструменты и методы используют,
4. и какие цели преследуют.

Тактики – что хочет сделать злоумышленник

Техники – как это делается. Также существуют **Sub-techniques** (уточнённые методы)

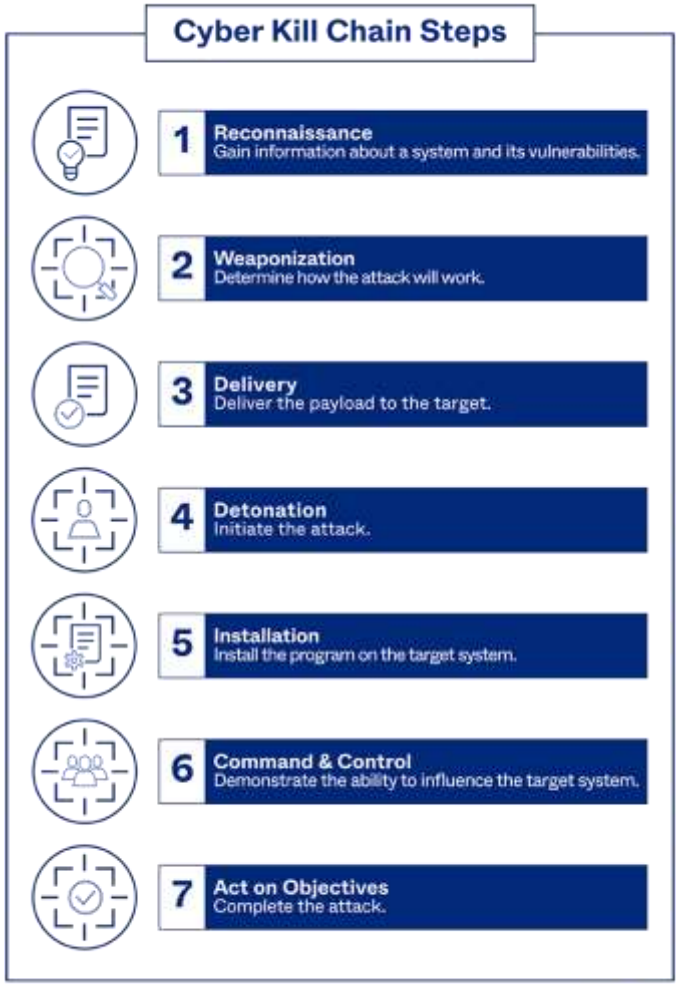
Методология KillChain

Разведка (*Reconnaissance*): Сбор информации о цели, используя OSINT, социальную инженерию и другие методы. Целью является выявление уязвимостей и слабых мест

Вооружение (*Weaponization*): Создание вредоносного ПО или эксплойта, который будет использоваться для атаки. Например, создание фишингового письма с вредоносным вложением

Доставка (*Delivery*): Доставка вредоносного ПО или эксплойта к цели. Например, отправка фишингового письма с вредоносным вложением сотруднику компании

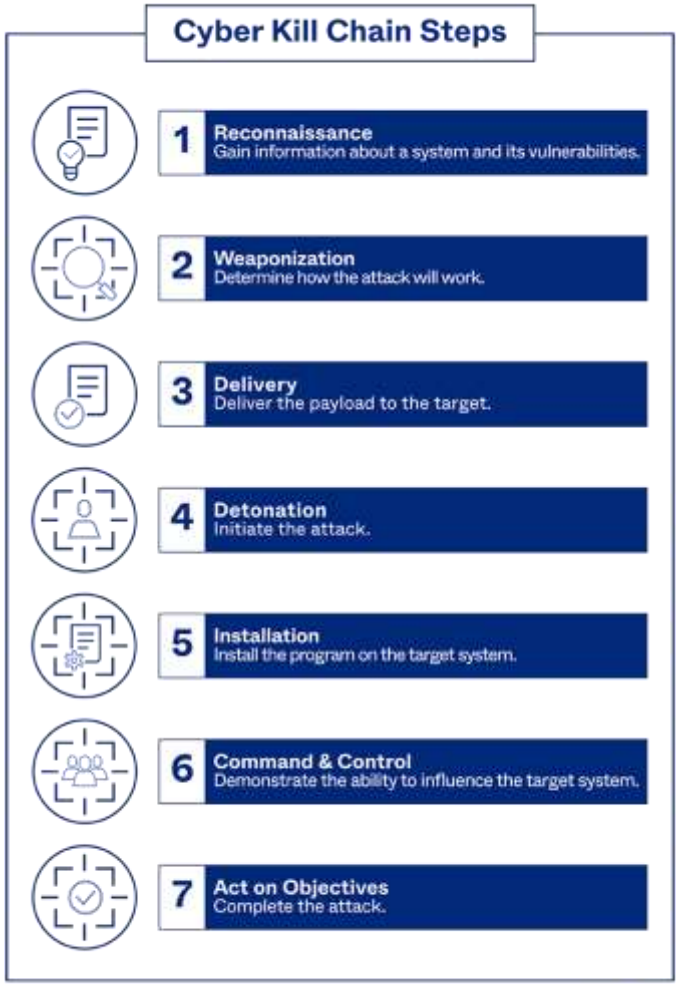
Эксплуатация (*Exploitation*): Использование уязвимости для выполнения вредоносного кода на целевой системе. Например, открытие вредоносного вложения в фишинговом письме приводит к выполнению кода на компьютере сотрудника.



Установка (*Installation*): Установка вредоносного ПО на целевой системе для получения постоянного доступа. Например, установка трояна для удаленного доступа (**RAT**) на компьютер сотрудника

Управление (*Command and Control*): Установление канала связи с зараженной системой для управления ею. Например, использование C2-сервера для отправки команд и получения данных с зараженного компьютера**.**

Действия на объекте (*Actions on Objectives*): Выполнение целей злоумышленника, таких как кража данных, уничтожение информации или распространение вредоносного ПО. Например, копирование конфиденциальных данных с сервера компании и отправка их на **C2-сервер**.



Отличия?

Отличия

MITRE ATT&CK – Это **реестр техник и поведения**, которые могут быть использованы **на любом этапе**, не обязательно последовательно

KillChain – Это **модель фреймворка атаки** — показывает, **как разворачивается атака по фазам**. Простая и последовательная