ЛЕКЦИЯ 1

Введение в область информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

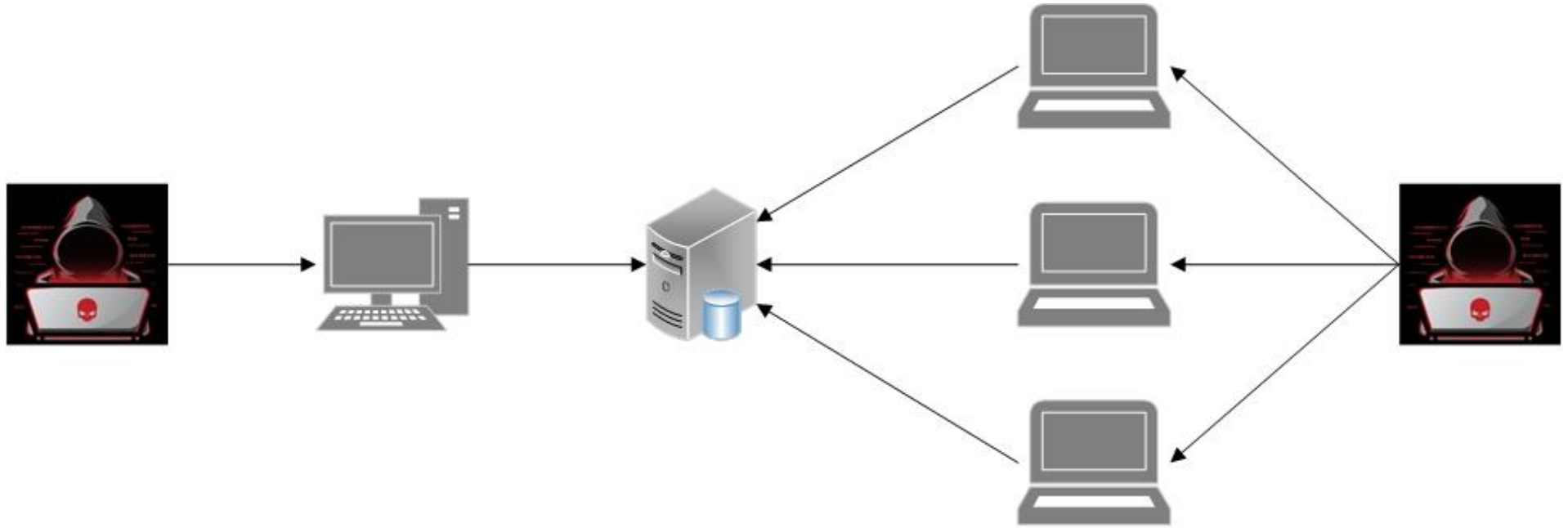
- Сегодня цифровые системы и технологии широко распространены во всех аспектах жизни. Поэтому кибератаки происходят очень часто. Обнаружение опасных программ и защита конфиденциальной информации всегда является актуальной проблемой и ключевым активом для экспертов по кибербезопасности.
- Количество киберпреступников и типов угроз в последнее время значительно возросло. Более того, кибератаки становятся все более сложными и запутанными, чем когда-либо. Для обеспечения защиты от таких кибератак действия по кибербезопасности направлены на защиту пользователей, их информационных систем, сетей и программ.
- Для развития кибербезопасности в Казахстане принимаются различные меры, в том числе концепция «Киберщит Казахстана», которая реализуется для решения проблемы кибератак.
- Кроме того, государственные и негосударственные организации совместно разрабатывают и совершенствуют методы кибербезопасности.
- В рамках мероприятия по информационной безопасности эксперты «Лаборатории Касперского» изучили наиболее распространенные киберугрозы в Казахстане в 2022 году. В прошлом году защитные веб-решения компании заблокировали 109183489 уникальных вредоносных объектов.
- Анализ этого года показывает, что наиболее распространенными киберугрозами являются спам-атаки и атаки вредоносного ПО, такие как фишинг и вредоносные документы, шпионское ПО и криптомайнеры.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КИБЕРУГРОЗЫ

- Существуют различные типы угроз и атак.
- Среди наиболее распространенных — отказ в обслуживании (DoS) и распределенный отказ в обслуживании (DDoS), Man-in-the-Middle (MiTM), SQL-инъекции, фишинг и вредоносное ПО.
- DoS и DDoS-атаки являются распространенными типами атак. DoS-атака — это кибератака, которая выводит из строя один компьютер или устройство, отправляя вредоносные файлы в систему, перегружая сеть и делая ее практически полностью недоступной.
- Это достигается путем отправки огромного объема трафика на веб-сайт, не давая ему отвечать другим законным пользователям. DDoS-атака осуществляется путем одновременной отправки вредоносных данных в систему через несколько устройств.
- Этот тип атаки трудно контролировать и блокировать, поскольку злоумышленник быстро отправляет поток трафика с нескольких устройств жертвам.
- Эти атаки представляют значительный риск для нескольких служб, поскольку атаки используют различные законные каналы для отправки сотен и тысяч сообщений, что затрудняет их блокировку.

DOS / DDOS

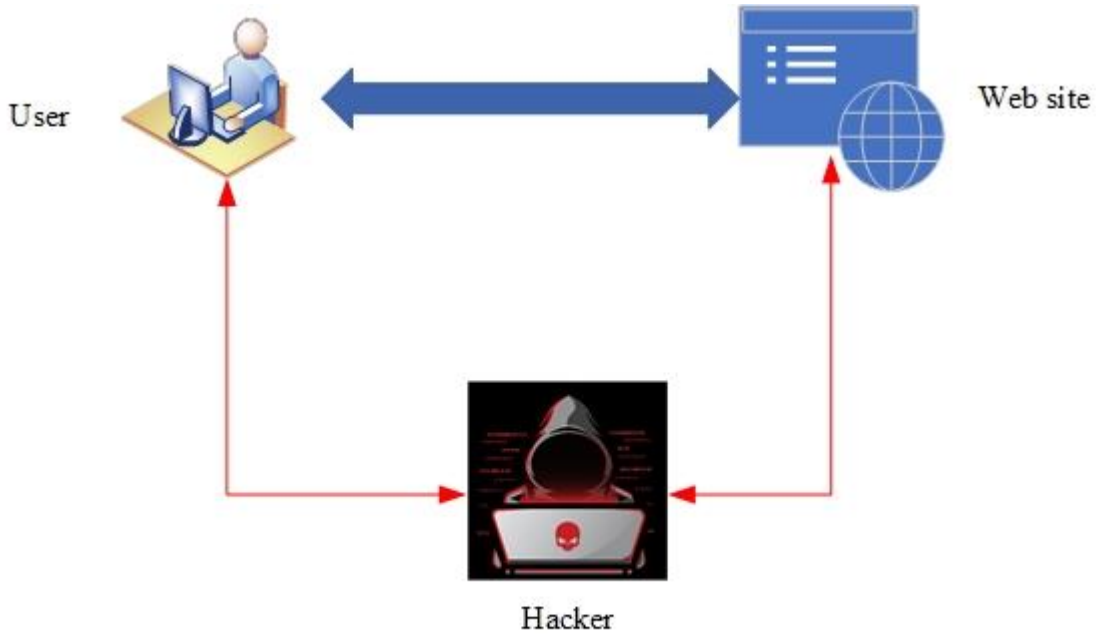


DoS and DDoS attacks

MAN IN THE MIDDLE

- Атака Man in the Middle — это атака, при которой злоумышленник перехватывает связь между двумя сторонами, оставаясь незамеченным для них обоих. В этом сценарии атака раскрывается только тогда, когда информация украдена. Злоумышленники могут получить доступ к информации, оставаясь в пассивной или активной роли. Пассивные злоумышленники тихо крадут данные банковских счетов, номера банковских карт или другую конфиденциальную информацию, будучи сторонним наблюдателем информации. В то же время активный злоумышленник становится участником, который эмулирует систему, изменяя содержание информации, переводя незаконные деньги или выдавая себя за ее законного участника. Пользователь веб-приложения или веб-сайта обменивается конфиденциальными данными, не замечая атаки, делая вид, что происходит законный обмен информацией.

MAN IN THE MIDDLE



Man in the Middle attack

PHISHING

- Фишинговая атака является одним из наиболее распространенных видов мошенничества с целью доступа к конфиденциальным данным пользователей. При этом типе атаки злоумышленник создает вредоносный веб-сайт, очень похожий на легитимный, и рассылает ссылки по разным каналам связи. Формы распространения фишинговых атак разнообразны. При электронном фишинге злоумышленники рассылают электронные письма и СМС с вредоносными ссылками. При поисковом фишинге злоумышленники конструируют нелегитимный веб-сайт, создавая ссылку, ведущую на него. Ссылки также продвигаются в поисковых системах с использованием распространенных механизмов индексации. Если пользователи открывают такие ссылки, они перенаправляются на конкретный веб-сайт, где мошенники достигают своей цели, получая доступ к ценным данным пользователей.

PHISHING

SQL ИНЪЕКЦИЯ

- Атака SQL-инъекцией является одной из самых распространенных и опасных кибератак, осуществляемых киберпреступниками для несанкционированного доступа к системам управления базами данных веб-приложений. Злоумышленники создают опасные SQL-коды для доступа и управления конфиденциальной информацией. Этот тип атаки может повлиять как на базовую структуру, так и на сами данные, включая ее последствия: раскрытие, кража, изменение, уничтожение конфиденциальных данных и полный взлом системы. Программа или код, которые наносят вред компьютерной системе, называются вредоносным ПО. Вредоносные программы обычно распространяются через Интернет и съемные устройства, такие как флэш-накопители. Они влияют на системы, снижая производительность компьютера, уменьшая свободное место на его HDD и SSD-дисках и выставляя на экране различные рекламные объявления. Такая ситуация явно свидетельствует о том, что компьютерная система пользователя заражена вредоносным ПО. Опасное вредоносное ПО продолжает выполнять вредоносные действия, похищая файлы с конфиденциальными данными и скрывая их внутри компьютера. Как правило, количество кибератак растет с каждым днем, и для их успешного обнаружения и предотвращения необходимо разрабатывать новые эффективные методы и модели.

SQL ИНЪЕКЦИЯ

СПАСИБО ЗА ВНИМАНИЕ!!!