ЗАЩИЩЕННОСТЬ И НАДЕЖНОСТЬ СОВРЕМЕННЫХ ОС

ПРЕЗЕНТАЦИЮ ПОДГОТОВИЛИ СТУДЕНТЫ ГРУППЫ 9ПКС-1.17:
СИРОДЖОВ Д.С, ТАНКОВ А.Д

ПЛАН ПРЕЗЕНТАЦИИ

- Понятие защищенной ОС
- Угрозы безопасности ОС
- Популярные атаки на ОС
- Подходы к построению защищенной ОС
- Методы защиты ОС
- Понятие надежности

ПОНЯТИЕ ЗАЩИЩЕННОЙ ОС

Операционная система называется защищенной, если она предусматривает средства защиты от основных классов угроз.

Защищенная ОС обязательно должна содержать средства разграничения доступа пользователей к своим ресурсам, а также средства проверки подлинности пользователя, начинающего работу с ОС. Кроме того, защищенная ОС должна содержать средства противодействия случайному или преднамеренному выводу ОС из строя.

Если ОС предусматривает защиту не от всех основных классов угроз, а только от некоторых, такую ОС называют частично защищенной.

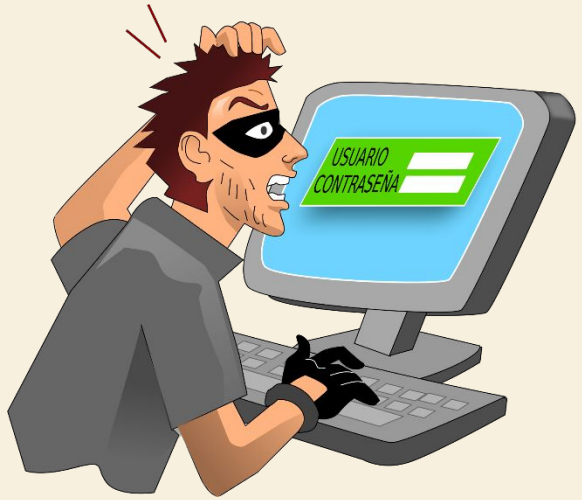
УГРОЗЫ БЕЗОПАСНОСТИ ОС

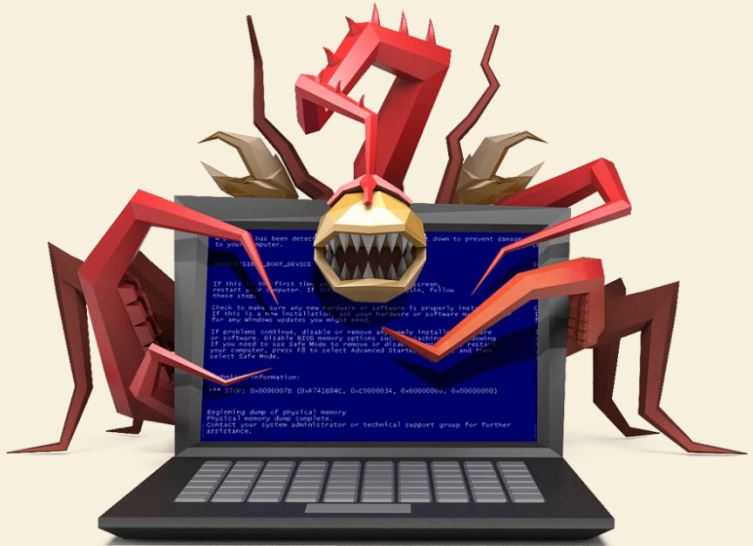
Угрозы безопасности ОС можно классифицировать по различным аспектам их реализации:

- По цели атаки
- По принципу воздействия на ОС
- По типу используемой уязвимости защиты
- По характеру воздействия на ОС

ПОПУЛЯРНЫЕ АТАКИ НА ОС

- Сканирование файловой системы. Злоумышленник просматривает файловую систему компьютера и пытается прочесть все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, который должен быть ему запрещен.
- Подбор пароля. Может использоваться как тотальный перебор пароля, так и подбор пароля с использованием знаний о пользователе.
- Кража ключевой информации. Злоумышленник может подсмотреть пароль, набираемый пользователем, или восстановить набираемый пользователем пароль по движениям его рук на клавиатуре. Носитель с ключевой информацией может быть просто украден.
- Жадные программы. Это программы, преднамеренно захватывающие значительную часть ресурсов компьютера, в результате чего другие программы не могут выполняться или выполняются крайне медленно. Запуск жадной программы может привести к краху ОС.
- Превышение полномочий. Злоумышленник, используя ошибки в программном обеспечении ОС или политике безопасности, получает полномочия, превышающие те, которые ему предоставлены в соответствии с политикой безопасности.





ПОДХОДЫ К ПОСТРОЕНИЮ ЗАЩИЩЕННЫХ ОС

Существуют два основных подхода к созданию защищенных ОС - фрагментарный и комплексный.

При применении фрагментарного подхода подсистема защиты ОС представляет собой набор разрозненных программных продуктов. Эти программные средства работают независимо друг от друга, при этом практически невозможно организовать их тесное взаимодействие. Кроме того, отдельные элементы такой подсистемы защиты могут некорректно работать в присутствии друг друга, что приводит к резкому снижению надежности системы.

При комплексном подходе защитные функции вносятся в ОС на этапе проектирования архитектуры ОС и являются ее неотъемлемой частью. Отдельные элементы подсистемы защиты, созданной на основе комплексного подхода, тесно взаимодействуют друг с другом при решении различных задач, связанных с организацией защиты информации, поэтому конфликты между ее отдельными компонентами практически невозможны.

МЕТОДЫ ЗАЩИТЫ ОС

- **Использование сложных паролей.** Такой метод хорошо защищает от так называемых «грубых» атак, суть которых заключается в применении злоумышленниками программ по автоподбору паролей.
- **Внешняя защита.** Даже в случае наличия всего лишь одного компьютера неплохо иметь и внешний брандмауэр/маршрутизатор.
- **Обновление программного обеспечения.** Долгое игнорирование появляющихся обновлений может привести к тому, что система станет легкой добычей для хакеров.
- **Отключение неиспользуемых служб.** Зачастую пользователи не знают, какие системные сетевые службы работают у них на компьютере. К примеру, Telnet и FTP часто весьма уязвимы для сетевых атак и должны быть отключены в случае, если они не используются.
- **Системы мониторинга нарушений и попыток атаки.** После проведения всех мер по защите системы не стоит терять бдительность и полагать, что теперь информация находится в полной безопасности. Следует постоянно выявлять подозрительные события на предмет взлома системы и хакерских атак.

ПОНЯТИЕ НАДЕЖНОСТИ

Надежность – это свойство объектов сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных условиях применения.

Интуитивно надёжность объектов связывают с недопустимостью отказов в работе. Это есть понимание надёжности в «узком» смысле — свойство объекта сохранять работоспособное состояние в течение некоторого времени или некоторой наработки. Иначе говоря, надёжность объекта заключается в отсутствии непредвиденных недопустимых изменений его качества на стадии эксплуатации

ИСТОЧНИКИ

- https://studopedia.ru/11_130623_bezopasnost-operatsionnih-sistem-sredstva-zashchiti-informatsii-v-seti.html
- https://studfiles.net/preview/5163176/page:2/
- https://vuzlit.ru/976768/ponyatie_zaschischennoy
- https://www.sites.google.com/site/bezopasnostos/
- https://studref.com/322475/informatika/obespechenie_bezopasnosti_operatsionnyh_sistem

СПАСИБО ЗА ВНИМАНИЕ!