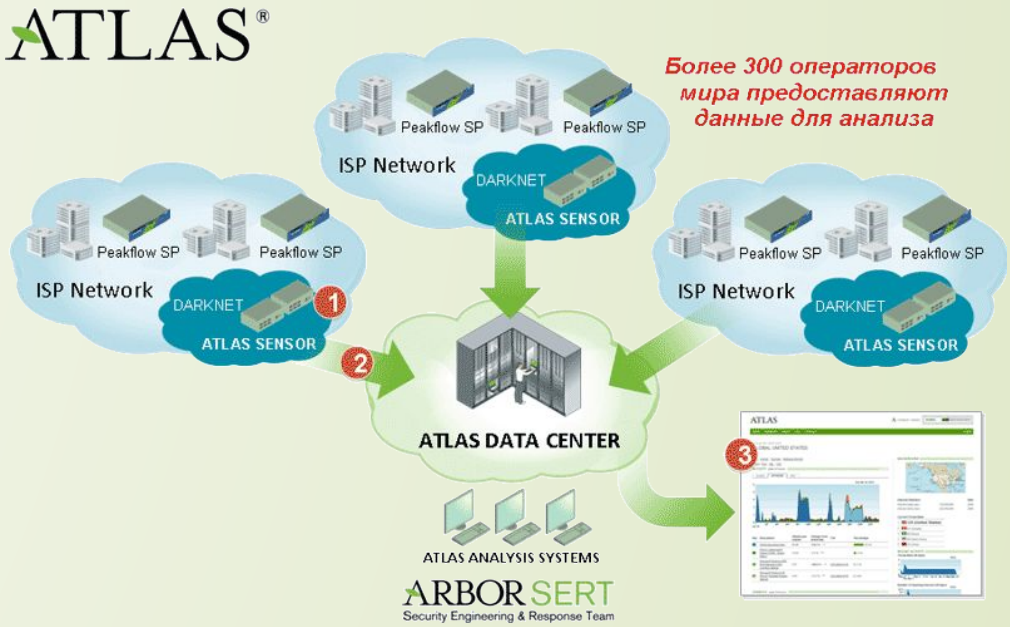
Хакерские утилиты и защита от них

11 класс

Сетевые атаки

- **Сетевая атака** – это попытка воздействовать на удаленный компьютер с использованием программных методов.
- **Цель сетевой атаки -** нарушение конфиденциальности данных, то есть, кража информации, получения доступа к чужому компьютеру и последующего изменения файлов, расположенных на нем.

Классификация атак:

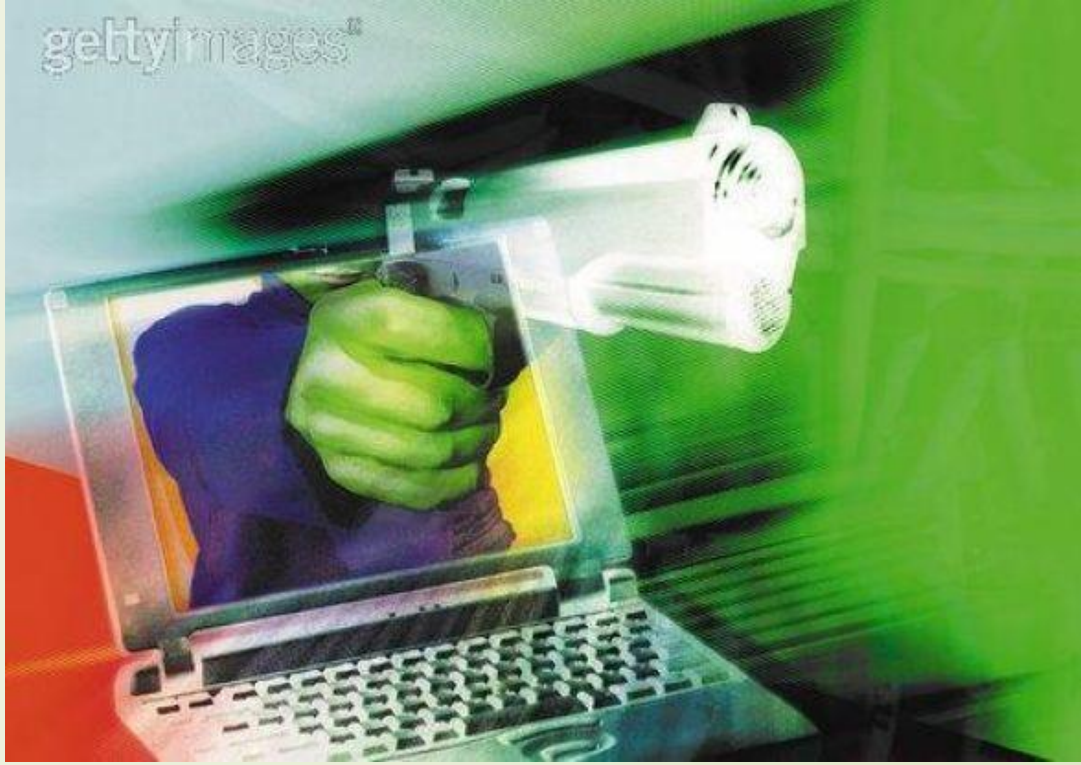


- **По характеру воздействия:**

1**. пассивное** - направлено на получение конфиденциальной информации с удаленного компьютера (чтение входящих и исходящих сообщений по электронной почте, прослушивание канала связи в сети.).

2**. активное** - их задачей является не только доступ к тем или иным сведениям, но и их модификация.

Классификация атак:

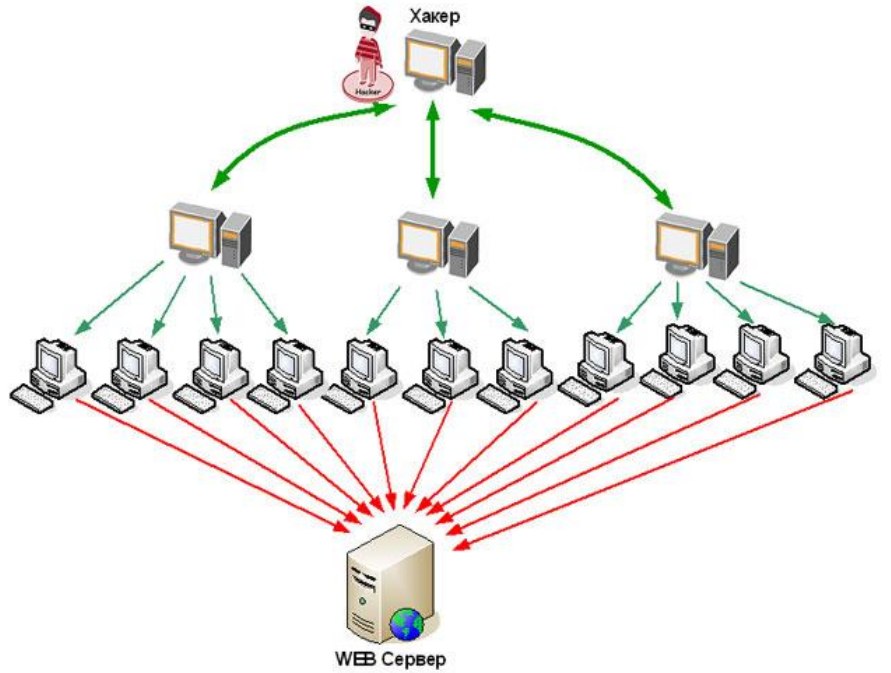


- **По цели воздействия**:

1. нарушение функционирования системы (доступа к системе)
2. нарушение целостности информационных ресурсов (ИР)
3. нарушение конфиденциальности ИР

Существуют два принципиальных варианта получения информации: искажение (полный контроль над потоком информации между объектами системы, либо возможность передачи различных сообщений от чужого имени -2) и перехват (нарушению ее конфиденциальности).

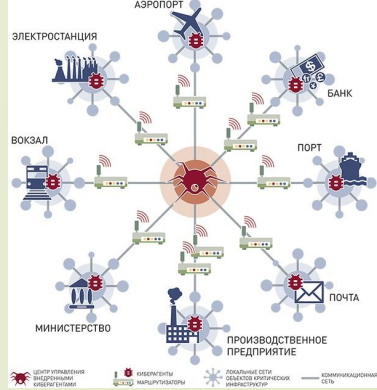
Классификация атак:



- **По наличию обратной связи с атакуемым ооъектом**

1. **с обратной связью** – отправляется запрос на атакуемый объект и ждет на него ответ (Подобные атаки наиболее характерны для распределённой вычислительной системы РВС).
2. **без обратной связи** (однонаправленная атака)- им не требуется реагировать на изменения на атакуемом объектею Примером однонаправленных атак является типовая УА «DoS-атака».

Классификация атак:



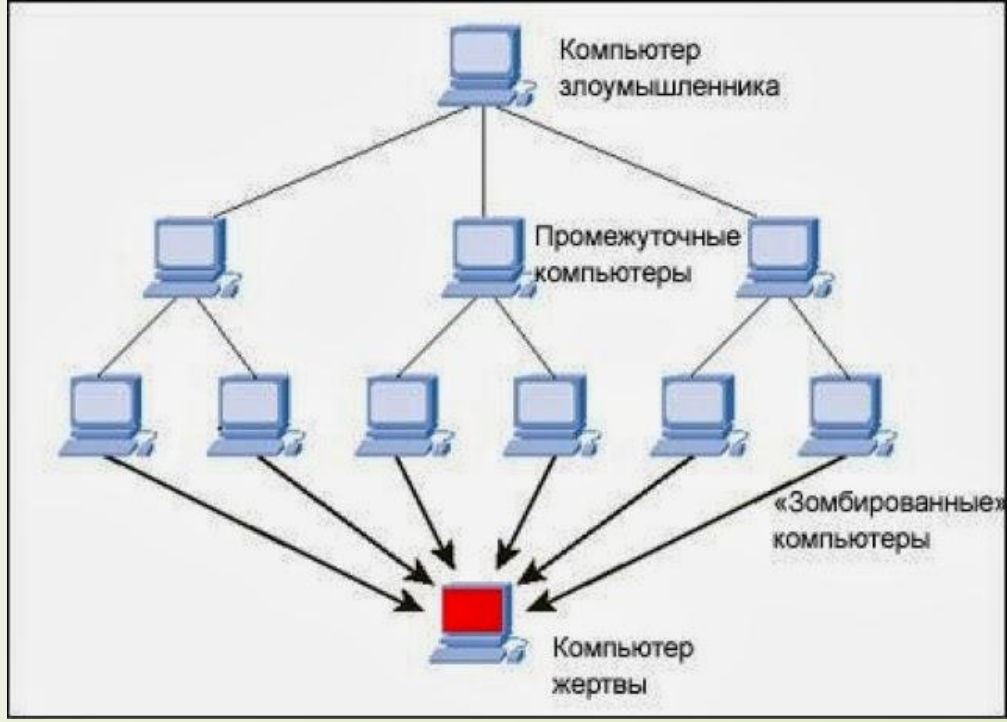
- **По условию начала осуществления воздействия**

1. **атака по запросу от атакуемого объекта** - Воздействие со стороны атакующего начнётся при условии, что потенциальная цель атаки передаст запрос определённого типа. Примером подобных запросов в сети Интернет может служить DNS- и ARP-запросы, а в Novell NetWare — SAP-запрос.
2. **атака по наступлению ожидаемого события на атакуемом объекте** - Атакуемый объект сам является инициатором начала атаки. Примером такого события может быть прерывание сеанса работы пользователя с сервером без выдачи команды LOGOUT в Novell NetWare.
3. **безусловная атака** - осуществляется немедленно и безотносительно к состоянию операционной системы и атакуемого объекта, атакующий является инициатором начала атаки, цель - вывод из строя ОС на атакуемом объекте и невозможность доступа для остальных объектов системы к ресурсам этого объекта. Примером атаки такого вида может служить УА «DoS-атака».

Технологии защиты

- Методы защиты от сетевых атак разрабатываются и совершенствуются постоянно, однако полной гарантии ни один из них не дает. Любая статичная защита имеет слабые места, так как невозможно защититься от всего сразу. Что же касается динамических методов защиты, таких как статистические, экспертные, защиты с нечеткой логикой и нейронные сети, то они тоже имеют свои слабые места, поскольку основаны преимущественно на анализе подозрительных действий и сравнении их с известными методами сетевых атак. Следовательно, перед неизвестными типами атак большинство систем защиты пасует, начиная отражение вторжения слишком поздно. Тем не менее, современные защитные системы позволяют настолько осложнить злоумышленнику доступ к данным, что рациональнее бывает поискать другую жертву.

Утилиты взлома удаленных компьютеров



- Предназначены для проникновения в удаленные компьютеры с целью дальнейшего управления ими или для внедрения во взломанную систему других вредоносных программ.
- Утилиты взлома удаленных компьютеров обычно используют уязвимости в операционных системах или приложениях, установленных на атакуемом компьютере.

Руткиты

- ***Руткит*** - программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредной активности. Также они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Защита от хакерских атак

1) Межсетевой экран позволяет:

• Блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);

• Не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);

• Препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

2) Своевременная загрузка из Интернета обновления системы безопасности операционной системы и приложений.

Домашнее задание:

§ 1.6.6, повторить главу 1.

выполнить конспект в тетрадь и ответить письменно на вопросы стр.99