Хакерские улиты и защита от них

Хакерские утилиты: что это?

способом могут нанести вред удаленному компьютеру

Что такое 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

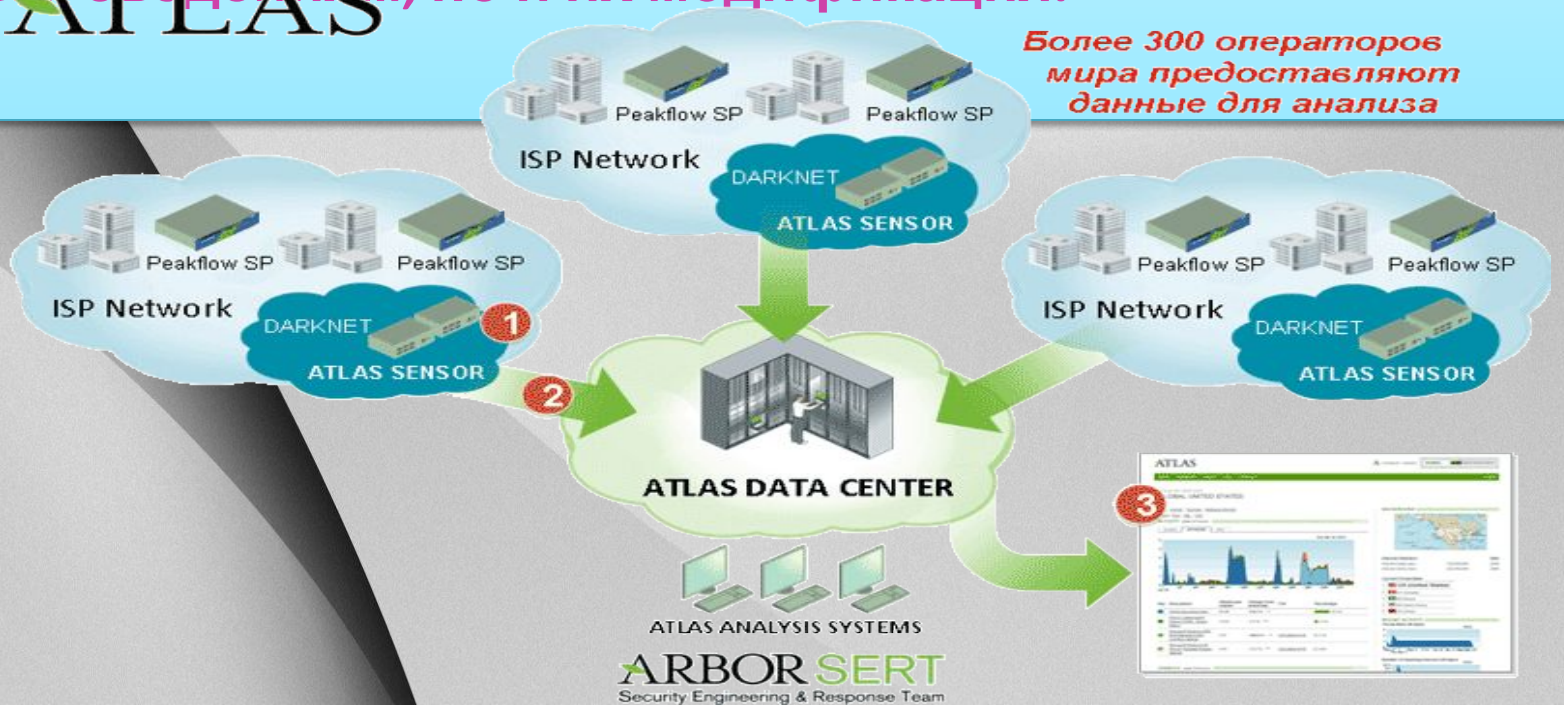
Классификация атак:

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.

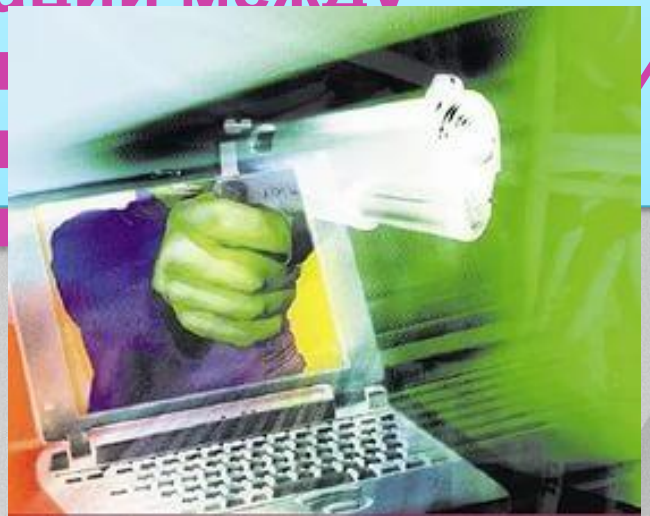
ATLAS®



Классификация атак:

По цели воздействия:

- нарушение функционирования системы (доступа к системе)
- нарушение целостности информационных ресурсов (ИР)
- нарушение конфиденциальности ИР
- Существуют два принципиальных варианта получения информации: искажение (полный контроль над потоком информации между объектами системы, либо возм и различных сообщений от чужо перехват (нарушению ее конфи



Классификация атак:

По наличию обратной связи с атакуемым объектом с обратной связью – ***отправляется запрос на атакуемый объект и ждет на него ответ (Подобные атаки наиболее характерны для распределённой вычислительной системы РВС).***

без обратной связи (однонаправленная атака)- им не требуется реагировать на изменения на атакуемом объектею Г

однонаправленных ат

«DoS-атака».

Классификация атак:

По условию начала осуществления воздействия

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.

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.

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

Технологии защиты

1. Любая статичная защита имеет слабые места, так как невозможно защититься от всего сразу.
2. Статистические, экспертные защиты с нечеткой логикой и нейронные сети 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.
3. Современные защитные системы позволяют настолько осложнить злоумышленнику доступ к данным, что рационал тву.

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.

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 бе стемы и приложений