Сценарии и модели сетевых атак и защиты на основе графов

Дескриптивная часть

Сценарии НВ

- Осуществление атак состоит из последовательности действий: действий, подготавливающих атаку, и действий, осуществляющих НВ.
  - **Подготовка атак:**
  - **Прослушивание сетевого трафика** (аутентификационные данные, пароль: противодействие = обнаружение запущенного сниффера)
  - **Сканирование уязвимостей** (учётные записи: противодействие = использование СОВ и анализ журналов регистрации МЭ)

Сценарии НВ

- **Сетевые атаки**:
- **- атаки, основанные на переполнении буфера** (overflows based attacks).
- Они используют уязвимость системы, заключающуюся в некорректной программной обработке данных. При этом появляется возможность выполнения вредоносного кода с повышенными привилегиями.
- **- атаки, направленные на отказ в обслуживании** (Denial Of Service attacks). Атаки не обязательно используют уязвимости в ПО атакуемой системы. Нарушение работоспособности системы происходит из-за того, что посылаемые ей данные приводят к значительному расходу ресурсов системы.

Сценарии НВ

- **Атаки, основанные на использовании уязвимостей в ПО сетевых приложений - эксплойты** (exploit).
- Данный класс атак основан на эксплуатации различных дефектов в ПО. Эксплойты представляют собой вредоносные программы, реализующие известную уязвимость в ОС или прикладном ПО для получения НСД к уязвимому хосту, или нарушение его работоспособности.
- Для эксплойтов характерно наличие функций подавления антивирусных программ и МЭ. Последствия применения эксплойтов могут быть самыми критическими. В случае получения злоумышленником удаленного доступа к системе, он имеет практически полный (системный) доступ к

Сценарии НВ

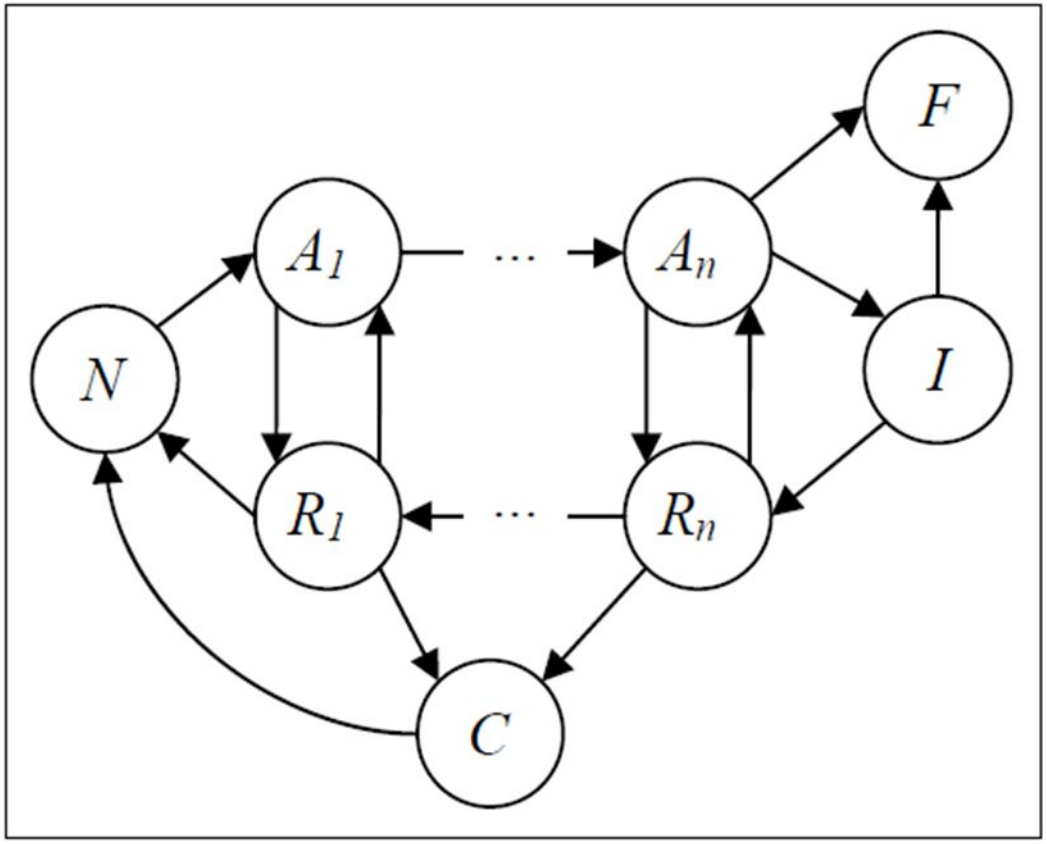
- Последующие действия и ущерб от них могут быть следующими: внедрение троянской программы, внедрение набора утилит для сокрытия факта компрометации системы, несанкционированное копирование злоумышленником данных с жестких и съемных носителей информации системы, заведение на удаленном компьютере новых учетных записей с любыми правами в системе для последующего доступа как удаленно, так и локально, кража файла с хэшами паролей пользователей, уничтожение или модификация информации, осуществление действий от имени пользователя системы.
- Противодействие=обновление СОВ и МЭ (обновление сигнатур вредоносных кодов).

Сценарии НВ

- **Вредоносные программы** – это компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в сети, либо для скрытого нецелевого использования ресурсов или либо иного воздействия, препятствующего нормальному функционированию сети. К ним относятся компьютерные вирусы, троянские кони, сетевые черви и др.
- Противодействие. Типичным методом противодействия является использование антивирусных средств, работающих в режиме реального времени (мониторов). Для выявления троянских программ существует специализированное программное обеспечение.

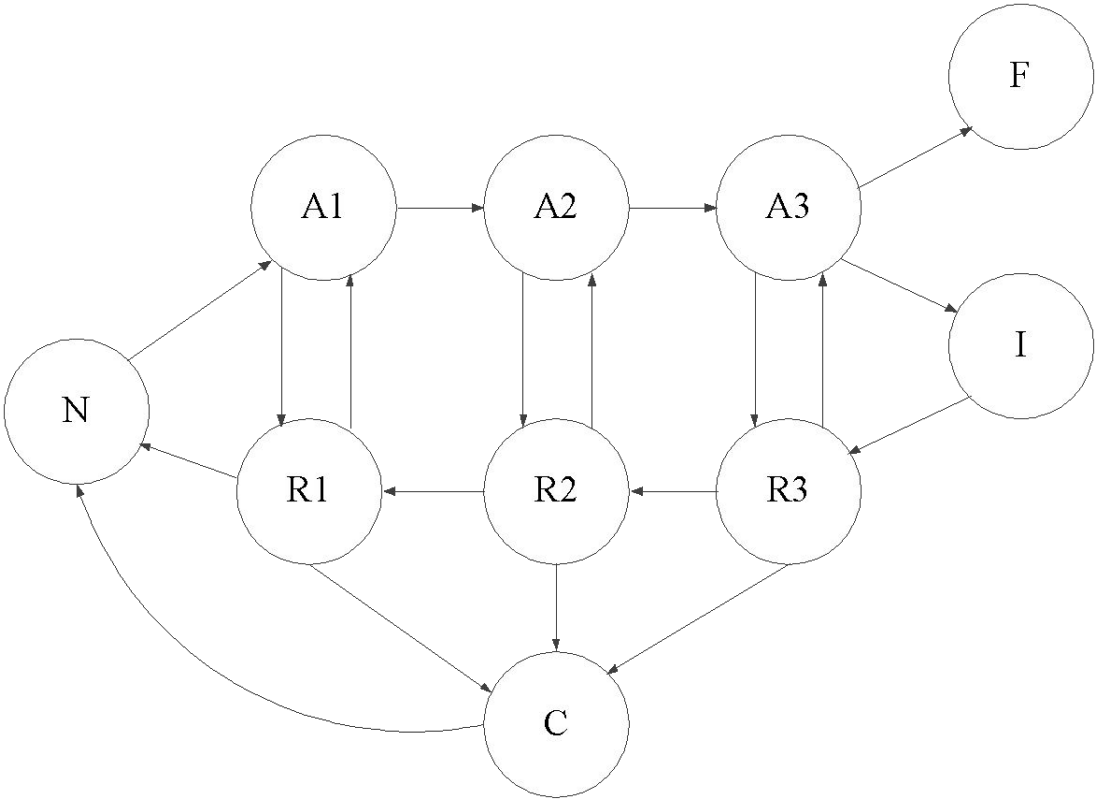

Начало атаки
Подготовка атаки
Прослушивание сетевого трафика
Сканирование уязвимостей
Атаки
Сетевые атаки
Атаки, основанные на переполнении буфера
Атаки, направленные на отказ в обслуживании
Эксплойты
Вредоносные программы

Марковская модель DOS-атаки



1.Норма (N) - обычный режим работы; 2.Атакуемый (Aj) - попытка несанкционированного доступа (НСД): 2.1.Прохождение 1-го слоя защиты; 2.n. Прохождение n-го слоя защиты; 3.Защита (Ri) - остановка НСД: 3.1. Восстановление n-го слоя защиты; 3.n. Восстановление 1-го слоя защиты; 4. Контратака (C) - блокировка угрожающего узла; 5.Отказ (F) - выход узла из строя; 6.Атакующий (I) - присоединение к группе атакующих узлов.

Пример разметки модели



- N – начальное состояние узла; A1 – прослушивание трафика; A2 – сканирование уязвимостей; A3 – НСД через внедрение эксплойта; R3 – защита НСД через СОВ и МЭ; R2 – защита от сканирования уязвимостей; R1 – защита от прослушивания трафика; C – блокировка атаки; F – отказ узла; I – присоединение узла к группе