XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.171

УДК 50.41.00

Е.А.Рудина (5 курс, каф. ИБКС), С.С.Корт, к.т.н., доц.

ПОДХОД К ОЦЕНКЕ ДИНАМИКИ РАЗВИТИЯ ВТОРЖЕНИЯ

Атака на компьютерную систему – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Под вторжением будем понимать нарушение безопасности, состоящее из одной или нескольких атак.

Методы, заложенные в основу большинства современных систем обнаружения вторжений, в общем случае не позволяют отследить динамику развития вторжения. Предлагается комплексный подход к выявлению вторжений, основанный на применении двух алгоритмов:

1) алгоритма, исследующего динамику развития вторжения в соответствии с типовыми сценариями, основанного на конечном автомате состояний, описывающего взаимосвязь различных этапов вторжения;
2) алгоритма, основанного на поиске аномалий.

Алгоритм анализа динамики развития вторжения анализирует состояние внешних станций по отношению к защищаемым серверам. При этом внешняя станция может быть охарактеризована следующим образом:

- неизвестная – обращавшаяся к защищаемому серверу в течение краткого периода времени,и не производившая атакующих действий;
- доверенная – обращавшаяся к защищаемому серверу в течение длительного периода времени и не производившая атакующих действий;
- подозрительная – производившая попытки сканирования или атаки защищаемого сервера, при этом успех сканирования/атаки оценивается на основании кодов возврата протоколов прикладного уровня, реализуемых защищаемыми сервисами.

Данные для анализа с использованием данного метода, управляющие переходами автомата, поступают от системы обнаружения атак «Snort».

С целью получения более точной оценки вторжения метод анализа динамики развития атаки был дополнен вторым алгоритмом – алгоритмом выявления аномалий, основой которого являются данные, образующие профиль поведения внешней станции по отношению к защищаемым сервисам. Если сценарий вторжения не был верифицирован, но было зафиксировано аномальное поведение удаленной станции по отношению к защищаемому сервису, то вторжение считается успешным, как и в случае верификации сценария.

Данный подход позволяет оценить сценарий развития вторжения, уменьшить число ложный срабатываний в обнаружении атак и предсказать возможные атаки на защищаемый сервер.