ПОДХОДЫ К ЗАЩИТЕ ЦЕЛЕВЫХ СИСТЕМ ОТ AET

Макеев Сергей Александрович
Финансовый университет при Правительстве РФ, Москва, студент
kzo-101@mail.ru

Актуальность

На сегодняшний день каждая организация имеет свою корпоративную сеть, в которой циркулирует информация разной степени важности, представляющая интерес для злоумышленника. Для обеспечения защиты корпоративных сетей от угроз строится многоуровневая система защиты, включающая в себя периметровые межсетевые экраны и VPN-коммутаторы, системы предотвращения вторжений. Такой подход к построению системы имеет право на жизнь, однако в 2010 компания Stonesoft объявила об открытии абсолютно новой категории угроз сетевой безопасности – динамических техниках обхода Advanced Evasion Techniques (AET). [1]

Техники AET предоставляют злоумышленникам своего рода мастер-ключ для доступа к любой целевой системе, например, к корпоративным ERP- и CRM-приложениям, SCADA-системам, путем обхода современных систем сетевой безопасности. В результате атаки компании могут понести значительный финансовый или репутационный ущерб. Весьма характерный пример последнего времени (2010) – в трояне ZeuS, созданном для кражи банковских данных и шпионажа, были заложены техники AET [2].

В статье приводится рассмотрение понятия динамических техник обхода, а также предложение по созданию комплексного решения обнаружения и отражения вторжений.

Методы обнаружения и предотвращения вторжений

Под системой предотвращения вторжений (СПВ, IPS) понимается программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Сетевые СПВ осуществляют сбор и анализ сетевых пакетов, на основании которых проводится обнаружение. Сенсоры таких систем могут быть распре-

делены по элементам сети. В данной статье рассматриваются именно сетевые СПВ.

Выделяют два основных подхода к обнаружению — обнаружение сигнатур (signature detection, misuse detection), обнаружение аномалий (anomaly detection) и гибридный подход. Основные методы обхода СПВ: сбивание с толку; фрагментация; шифрование; перегрузка. [3]

Классический подход к безопасности сети неспособен динамически выявить новые атаки. В статичных методах сигнатурного или шаблонного обнаружения уже недостаточно простого «отпечатка».

Специфика техник обхода

Статья «Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection» об атаках против сетевых систем обнаружения вторжений появилась в 1997 г. Согласно статье, техники обхода есть средство доставки любого «полезного груза» до целевой системы без ее обнаружения средствами сетевой защиты (СПВ).

Необходимо отметить, что большинство техник обхода используют мягкие требования к интерпретации работы протоколов и обычно не нарушают стандартов RFC, поэтому модули разбора протоколов их также не распознают. Примером известных техник обхода являются: IP fragmentation, MSRPC encryption, TCP segmentation, MSRPC fragmentation, SMB fragmentation, TCP TIME_WAIT, IP random options и др. [4]

Динамические техники обхода (АЕТ) – это развитие традиционных техник обхода, которые базируются на следующих принципах: [1]

- объединение нескольких способов обхода, которые действуют на различных уровнях сетевого взаимодействия;
- использование не декларированных и редко используемых свойств протокола;
- возможность изменить комбинацию техник обхода во время атаки;
- продуманное построение атак.

Для маскировки «полезного груза» АЕТ используют слабые места протоколов, а также невысокие ограничения по безопасности при сетевой коммуникации. Так можно внедрять пакеты данных, которые кажутся безвредными для СПВ и проявляют себя как атака только при их интерпретации целевой системой.

Эксперты из компании Stonesoft с конца 2010 года выявили 147 различных видов АЕТ. [1]

Подходы к созданию систем предотвращения вторжений

Большинство современных средств защиты лишь приближается к тому, чтобы максимально быстро закрывать уязвимости. Для реального комплексного подхода необходимо детектировать атаку по контентному содержанию пакетов и анализу используемых эксплойтов.

Для защиты целевых систем от применения АЕТ необходимо скорректировать принципы построения СПВ:

1) нормализация IP/TCP-трафика;
2) наблюдение и анализ на всех уровнях протоколов;
3) восстановление фрагментированных IP-пакетов до их анализа;
4) обнаружение, основанное на изучении трафика на уровне приложений модели OSI;
5) статистический анализ данных;
6) возможность обучения и самообучения (встроенные тесты на проникновение).

Наиболее существенная защита против АЕТ – это нормализация протоколов. СПВ должна инспектировать и анализировать весь сетевой трафик по набору сигнатур, чтобы любая незнакомая и потенциально опасная последовательность данных могла быть легко идентифицирована, а ее распространение по сети – своевременно предотвращено. Однако это очень сложный процесс, и если нормализация протоколов не будет в полной мере реализована, эксплойты смогут «пройти» через систему безопасности.

Выводы

Динамическим техникам обхода сложно противодействовать именно потому, что они комбинированные и имеют большую вероятность успеха, в отличие от одиночных применений.

Для динамических угроз сетевой безопасности системы защиты необходимо постоянно обновлять, чтобы не отставать от процесса совершенствования угроз. Для этого чрезвычайно важно проводить детальный анализ методов нападения и понимать, какие уязвимости системы эксплуатировались.

Список источников

1. Multilayer Traffic Normalization and Data Stream Based Inspection: Essential Design Principles of the Stonesoft IPS. Whitepaper. – 2012.

2. Тараканов Д. За кем охотится ZeuS. http://www.securelist.com/ ru/analysis/208050628/Za_kem_okhotitsya_ZeuS. – 2010.

3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования / В.В.Платонов. — М.: Издательский центр «Академия», 2013. — 336 с. (Сер. Бакалавриат).

4. Network Intrusion: The Advanced IPS Evasion Techniques. http://basicnetworkingconcepts.blogspot.ru/2011/02/network-intrusion-advanced-ips-evasion.html. - 2011.