СУЩЕСТВУЮЩИЕ МЕТОДЫ И МОДЕЛИ УЯЗВИМОСТЕЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

Шамшиева Барно Махмуджановна

https://doi.org/10.5281/zenodo.7857752

Аннотация. *В статье рассматривает различные типы уязвимостей, методы и модели, используемые для выявления и исследования уязвимостей в компьютерных сетях. Описываются признаки уязвимостей, а также сравниваются различные уязвимости на основе их характеристик. В статье рассмотрены существующие модели уязвимостей, используемые для выявления и анализа уязвимостей в компьютерных сетях.*

Ключевые слова: *компьютерные сети, уязвимость, типы уязвимостей, сканирование портов, протоколы, сканирование портов, анализ журнила, проверка безопасности, тестирование.*

Компьютерные сети являются неотъемлемой частью современной информационной технологии. Однако, с ростом числа пользователей и компьютерных систем, сетевые уязвимости становятся все более распространенными. Уязвимости могут привести к различным проблемам, таким как нарушение конфиденциальности данных, нарушение целостности данных и отказ в обслуживании. В этой статье рассматриваются различные типы уязвимостей, методы и модели, используемые для выявления и исследования уязвимостей в компьютерных сетях.

Типы уязвимостей. Существует множество различных типов уязвимостей, которые могут присутствовать в компьютерных сетях. Некоторые из них включают:

Уязвимости веб-приложений. Нарушение контроля доступа (Broken Access Control), Сбои в криптографии (Cryptographic Failures), Внедрение кода (Injection), Небезопасный дизайн (Insecure Design), Неправильная конфигурация (Security Misconfiguration)

Уязвимости операционных систем. Уязвимости в операционных системах (ОС) или приложениях имеют следующее происхождение:

- Программные ошибки. Ошибка в программном коде может позволить вредоносной программе получить доступ к устройству и взять его под контроль.
- Функции, предусмотренные при разработке ОС

Уязвимости сетевых протоколов. Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

Уязвимости баз данных. Уязвимостью может быть неточность в конфигурации системы, например, отсутствие политики паролей базы данных, ошибка в программной части, например, переполнение буфера в какой-либо процедуре, или ошибка в настройке управления доступом, например, наличие публичных прав доступа к таблице, содержащей конфиденциальную информацию

Уязвимости браузеров. Нарушения безопасности веб-браузера обычно имеют целью обход средств защиты для отображения всплывающей рекламы, сбора личной информации (PII) либо для интернет-маркетинга либо для кражи личных данных, отслеживания веб-сайтов или веб-аналитики о пользователе против его воли с использованием инструментов,

таких как веб-маяк, Кликджекинг, Likejacking, HTTP cookie, зомби cookie или файлы Flash cookie Flash cookies (локальные общие объекты или LSO); установка рекламного ПО, вирусы, шпионское ПО таких как троянские программы (для получения доступа к персональным компьютерам пользователей путем взлома) или другое вредоносное ПО, включая кражу интернет-банкинга с использованием атак «Человек-в-браузере».

Уязвимости виртуальных машин. Каждый тип уязвимости имеет свои характеристики и способы выявления.

Сравнение уязвимостей. Различные уязвимости можно сравнить на основе их характеристик, таких как тип атаки, тип уязвимости, уровень угрозы, наличие патчей, доступность эксплоитов и т.д. Некоторые уязвимости более опасны и трудны для обнаружения, в то время как другие могут быть легко исправлены.

Выявление уязвимостей. Для выявления уязвимостей в компьютерных сетях используются различные методы, такие как: сканирование портов, анализ уязвимостей, анализ журналов, проверка безопасности приложений, тестирование на проникновение, использование средств интеллектуального анализа данных.

Каждый из этих методов имеет свои преимущества и недостатки, а также может использоваться для выявления различных типов уязвимостей.

Признаки уязвимостей. Уязвимости в компьютерных сетях могут иметь различные признаки, которые помогают в их выявлении. Некоторые из признаков уязвимостей включают:

- Ошибки в коде программного обеспечения
- Неправильно настроенные настройки безопасности
- Уязвимости в процессе аутентификации
- Наличие уязвимых компонентов

Программная ошибка — означает ошибку в программе или в системе, из-за которой программа выдает неожиданное поведение и, как следствие, результат. Большинство программных ошибок возникают из-за ошибок, допущенных разработчиками программы в её исходном коде, либо в её дизайне. Также некоторые ошибки возникают из-за некорректной работы инструментов разработчика, например из-за компилятора, вырабатывающего некорректный код.

Настройки безопасности и предотвращение опасных ситуаций. Например, если принтер подключен к сети, можно получить к нему доступ из удаленного местоположения. Кроме того, сразу несколько пользователей смогут совместно использовать этот принтер, что позволяет повысить эффективность и удобство работы. При этом, однако, увеличиваются такие риски, как незаконный доступ, нелегальное использование и взлом данных. При использовании принтера в среде, где есть доступ к Интернету, риски растут еще больше.

Уязвимости в процессе аутентификации. На основе функциональных особенностей клиентского приложения, входящего в информационные системы, проводится построение концептуальной модели угроз информационной безопасности информационных систем, которая применяется для выявления и исследования возможных атак на процесс аутентификации пользователей. В результате выявления критических мест безопасности системы, формируются основные требования, соблюдение которых позволит повысить

состояние защищенности систем, а именно: необходимость обеспечения подлинности и целостности ЭВМ, принимающих участие в процессе аутентификации пользователей в приложении, необходимость обеспечения конфиденциальности передаваемых и хранимых аутентифицирующих данных пользователей. Результаты данной работы позволяют обезопасить процесс аутентификации с использованием технологи Active Directory, а также проводить дальнейшие исследования в области аутентификации пользователей в распределенных системах. Проведенный анализ позволяет сделать вывод о безопасности применения предложенного способа аутентификации при соблюдении выявленных требований.

Наличие уязвимых компонентов. Для технологии характерны процедуры быстрого обнаружения, ранжирования и подтверждения подлинности источников первичных сообщений о таких проблемах. Технология основана на сборе и добыче информации об ошибках, уязвимостях и эксплойтах, содержащейся в сообщениях, опубликованных в источниках разработчиков открытого программного обеспечения. Технология включает процедуру подтверждения информации о наиболее опасных уязвимостях с последующей оценкой риска подтвержденных уязвимостей.

Идентификация этих признаков может помочь в обнаружении уязвимостей до того, как они будут использованы злоумышленниками.

Существующие модели уязвимостей. Существует множество различных моделей уязвимостей, используемых для выявления и анализа уязвимостей в компьютерных сетях. Некоторые из наиболее распространенных моделей включают:

Модель CVE (Common Vulnerabilities and Exposures)

Модель CVSS (Common Vulnerability Scoring System)

Модель CWE (Common Weakness Enumeration)

Каждая из этих моделей предоставляет средства для классификации и анализа уязвимостей в компьютерных сетях.

В заключении можно сказат что уязвимости в компьютерных сетях могут представлять серьезную угрозу для безопасности информации и требуют непрерывного мониторинга и анализа. Различные методы и модели, описанные в этой статье, могут помочь в выявлении и анализе уязвимостей в компьютерных сетях. Регулярное сканирование и анализ уязвимостей в компьютерных сетях является важным шагом для поддержания безопасности информации и защиты от кибератак.

REFERENCES

1. D. Kennedy et al., "Penetration Testing: A Hands-On Introduction to Hacking," 2nd ed., No Starch Press, 2014.
2. R. K. Lippmann et al., "Penetration Testing: Procedures & Methodologies," SANS Institute, 2015.
3. P. Mell et al., "The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems," National Institute of Standards and Technology, 2016.
4. S. S. Manadhata and J. Wing, "An Attack Surface Metric," IEEE Transactions on Software Engineering, vol. 37, no. 3, pp. 371-386, May-June 2011.

5. M. Bishop, "Common Weakness Enumeration," IEEE Security & Privacy, vol. 7, no. 1, pp. 78-81, Jan.-Feb. 2009.
6. J. A. Halderman et al., "A Measurement Study of the HTTPS Certificate Ecosystem," Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain, Oct. 2013, pp. 329-342.
7. N. Nikiforakis et al., "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting," Proceedings of the 2013 IEEE Symposium on Security and Privacy, San Francisco, CA, May 2013, pp. 541-555.