УДК 681.321

Алаа Мохаммед Абдул-Хади

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков

ОЦЕНКА ИНТЕНСИВНОСТИ АТАК НА УЯЗВИМОСТИ ДОСТУПНОСТИ КОММЕРЧЕСКИХ ВЕБ-СЕРВИСОВ

В статье рассмотрены вопросы оценки интенсивности атак на доступность коммерческих веб-сервисов и их элементов. Проведен анализ лиц, выполняющих атаки, их целей и мотивов, средств эксплуатации уязвимостей. Выдвинута гипотеза о марковости процессов, обусловленных событиями проведения атак на веб-сервис. Разработана модель расчета интенсивности атак на веб-сервис и его элементы, на основании ее определена интенсивность и критичность атак на доступность служб dns.

Ключевые слова: *интенсивность атак, уязвимости доступности, коммерческий веб-сервис, марковские модели.*

Введение

Успешный ввод и эксплуатация коммерческого веб-сервиса возможны только при условии окупаемости затрат на его функционирование и получения прибыли. При этом точка окупаемости достигается после введения сервиса в эксплуатацию, а при неправильной оценке рисков вообще может быть не достигнута. Это обуславливает важность моделирования функционирования веб-сервиса с учетом актуальных рисков киберобстановки [1].

Большинство веб-сервисов испытало на себе атаки различного рода. Что касается коммерческих веб-сервисов, они являются наиболее привлекательной целью для проведения атак [2]. В таких условиях актуализируется необходимость моделирования атак на веб-сервис как событий, обуславливающих его неработоспособность (а точнее – недоступность). Однако, большинство известных моделей атак, угроз и инцидентов имеют вероятностный характер оценки рисков. Лишь в некоторых источниках указывается на возможность моделирования веб-сервиса с помощью марковских или полумарковских процессов и аппарата сетей Петри [3].

Такая ситуация вызвана, прежде всего, сложностью получения первичных параметров временных моделей – интенсивностей проведения атак. К сожалению, большинство веб-сервисов скрывают статистику атак для сохранения репутации компании или бренда.

Возможно три направления решения задачи определения интенсивности атак:

– получение, обобщение и анализ скрытой информации об атаках на веб-сервисы;

– моделирование атак с помощью игровых методов и соревнований [4];

– исследование и анализ доступной информации об отдельных элементах механизма проведения атаки (в частности, об уязвимостях веб-сервиса и его элементов) [5].

Первое направление исследований практически затруднено. Что касается игрового метода, то проводимые исследования [4] дают хорошую характеристику формы и законов распределения времени между случайными событиями – атаками, однако не позволяют получить их количественные характеристики для конкретных систем. Поэтому в данной работе рассматривается последнее направление – получение количественных характеристик интенсивности атак, исходя из доступных данных об уязвимостях веб-сервисов и их элементов.

Следует отметить, что некоторые эксперты высказывают резкую критику относительно такого подхода [6]. Однако, эта критика конструктивна только в части методов оценки размерности множества уязвимостей отдельных программных продуктов и их сравнения между собой [7].

Постановка задачи исследования. Рассмотрим классическую схему таксономии компьютерных и сетевых инцидентов [8], включающую атаки (рис. 1).

Ключевым элементом в изображенной последовательности являются уязвимости системы. Атаки проводят на уязвимые системы (или с использованием обнаруженных уязвимостей). Если в системе нет уязвимостей, то атаки на нее безрезультатны. Современные коммерческие веб-сервисы являются сложными распределенными многокомпонентными системами, поэтому вероятность отсутствия в них уязвимостей бесконечно мала (стремится к нулю).

Возникают вопросы: насколько критичны уязвимости для функционирования веб-сервиса и как часто их будут эксплуатировать атакующие?

Ответ на первый вопрос можно найти в репозиториях уязвимостей, поддерживающих систему оценки CVSS, в которой фиксируется экспертная оценка критичности каждой уязвимости и ее влияние на конкретный подэлемент информационной безопасности (в данной работе рассматривается только уязвимости на доступность).

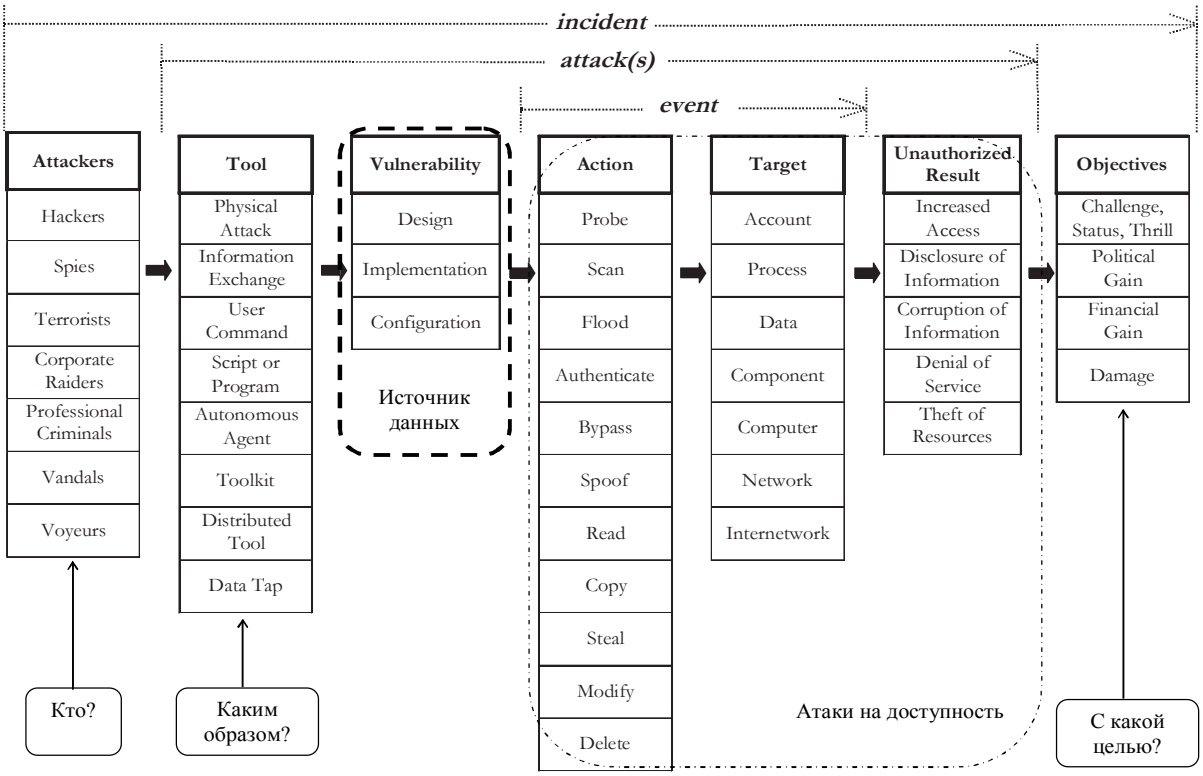

Рис. 1. Таксономия сетевых и компьютерных инцидентов, включающая атаки и уязвимости

Чтобы ответить на второй вопрос, необходимо еще раз проанализировать, кто, с какой целью и каким образом «эксплуатирует» уязвимости доступности веб-серверов и их элементов.

Таким образом, **целью данной статьи** является разработка метода оценки интенсивности атаки на веб-сервис на основе доступных данных из репозиториев уязвимостей.

Основная часть

Анализ лиц, эксплуатирующих уязвимости и средств из эксплуатации

Известны достаточно полные и емкие таксономии, позволяющие точно определить характеристику атакующих лиц и их инструментария. Выделяют следующие категории атакующих [8]:

– сотрудники;
– специалисты (хакеры);
– конкуренты;
– террористы;
– профессиональные преступники;
– спецслужбы государств.

По уровню подготовки, как правило, выделяют три группы (низкий, средний, высокий). По уровню организованности – одиночки и организованные группы. Также применимы и другие критерии.

Приведем пример выборки из таксономии [8]:

– хакеры-одиночки, класс 1 (ресурсы ограничены, креатив – средний, обнаруживаемость – высокая, численность – множество, цели – меняются, организованность – нет);

– хакеры-академики, класс 2 (ресурсы средние, креатив – высокий, обнаруживаемость – высокая, численность – средняя, цели – публичность, организованность – нет);

– организованные преступники, класс 3 (ресурсы неограниченны, креатив – средний, обнаруживаемость – низкая, численность – несколько, цели – деньги, организованность – да);

– государство, класс 3 (ресурсы неограниченны, креатив – средний, обнаруживаемость – низкая, численность – неизвестно, цели – меняются, организованность – да).

Характеристика инструментариев эксплуатации уязвимостей хорошо показана в [7], где она коррелируется со сложностью атаки:

– уровень 1 – инструментов и знаний не надо, может произойти случайно;

– уровень 2 – минимальные знания, универсальные инструменты;

– уровень 3 – техническая подкованность требуется, инструменты можно найти в Интернет;

– уровень 4 – инженерная подготовка, редко используемые или специфичные инструменты;

– уровень 5 – специально разработанные инструменты, академическая подготовка;

– уровень 6 – моделирование в лаборатории.

Анализ причин проведения атак на веб-сервисы

В [8] выделены следующие причины, или цели, которые преследуются атакующими при эксплуатации уязвимостей: шутка; хулиганство; любопытство; самоутверждение; известность и слава; месть и недо-

вольство; финансовая выгода; политика и идеология. Также следует отметить, что по целенаправленности атаки могут быть прямыми и косвенными. Под прямой атакой понимают действия атакующего только на целевой один веб-сервер. Примером косвенных атак могут служить атаки на доменные зоны отдельных государств (теракты или действия спецслужб) либо атаки на хостинг, где размещено множество веб-серверов (конкуренция служб хостинга).

Определенным образом на вероятность того, что веб-сервер станет объектом целевой атаки, влияет его прибыльность. Она может быть определена злоумышленником по явным признакам (например, через сотрудников бухгалтерии или информацию из налоговых баз) или по косвенным признакам (коммерческий характер деятельности, рост количества посетителей сервиса и др.).

Гипотеза о марковости процессов, обусловленных событиями проведения атак на веб-сервис

На основе конкретизации определенного вида атаки по действующему лицу, инструментарию, уязвимости и цели можно судить о ее случайном либо регулярном характере. Однако, в моделях готовности и доступности веб-серверов исследуется влияние не одной, а множества атак на доступность. Как видно из проведенного анализа, эти атаки могут иметь различную мотивацию, количество атакующих и целенаправленность. В силу известной теоремы о марковости (простейшем потоке событий) процесса, образованного из множества независимых потоков [9], в работе выдвинута гипотеза о том, что поток событий, обусловленных множеством атак на доступность как веб-сервера, так и его элементов – простейший.

Механизмы фиксации информации об уязвимости в репозитарии

Очевидно, что вероятность того, что уязвимость будет эксплуатироваться (а соответственно и интенсивность атак) прямо зависит от доступности информации о ней. Введем следующую классификацию хранилищ информации об уязвимостях:

0) уязвимость присутствует в программном продукте, но никем не обнаружена (информация о ней недоступна никому);

1) «хранилища черной зоны» – уязвимость обнаружена, но информация про нее доступна частному лицу либо организации закрытого типа (информация доступна узкому ограниченному кругу лиц);

2) «хранилища серой зоны» – уязвимость обнаружена, информация про нее выложена на закрытые форумы с ограниченным числом подписчиков;

3) «хранилища белой зоны» – открытые репозитарии уязвимостей (информация доступна всем);

4) уязвимость обнаружена (была «проэксплуатирована») и устранена.

Рассмотрим механизмы попадания уязвимости в открытые репозитарии:

а) «0-3-4» – уязвимость обнаружена доброжелателем и сразу зафиксирована в открытом репозитарии;

б) «0-1-4-3» – уязвимость была обнаружена злоумышленником, который ее успешно использовал, после ее устранения данные занесены в открытый источник;

в) «0-1-2-4-3» – уязвимость обнаружена злоумышленником, через некоторое время информация о ней размещена в хранилище серой зоны, далее уязвимость была успешно использована, а после ее устранения информация про нее занесена в открытый репозитарий;

г) «0-1-2-3-4» – уязвимость обнаружена злоумышленником, через некоторое время информация о ней размещена в хранилище серой зоны, далее доброжелатели с доступом к хранилищу передают информацию про уязвимость в открытый репозитарий.

Рассмотренные механизмы влияют на длительность временного промежутка между обнаружением уязвимости и внесением информации о ней в репозитарий. При этом, как отмечают исследователи [5], большинство уязвимостей имеют относительно короткий период обнаружения и фиксации информации в 59 суток.

Модель расчета интенсивности атак на веб-сервис и его элементы

Как было показано в [10], открытый репозитарий содержит информацию, позволяющую формировать подмножества уязвимостей на доступность элементов веб-сервера исходя из их критичности. Полученное подмножество включает также временные моменты внесения информации (Published).

Так как информация про уязвимости равновероятно может поступить в базу как от специалистов по безопасности (доброжелателей), так и после их эксплуатации злоумышленниками, то время регистрации уязвимости отображает степень заинтересованности конкретным элементом веб-сервера исследователями. Очевидной является тенденция постепенного затухания интереса к устаревшим версиям программных продуктов.

На основании проведенного анализа в работе принято допущение о том, что интенсивность атак на доступность конкретного элемента веб-сервера можно определить как максимальное значение усредненной за год частоты фиксации информации об уязвимостях, которые могут быть использованы для выполнения подобных атак. При этом критичность атаки определяется как средняя величина базовой оценки CVSS. Последовательность расчета интенсивности атак на доступность следующая:

1) составление структурной схемы веб-сервиса, включающей последовательно-паралельные соединения элементов, влияющих на доступность (по аналогии со структурной схемой надежности);

2) формирование подмножеств (выборок) уязвимостей на доступность элементов веб-сервиса;

3) определение значений усредненной за год частоты фиксации информации об уязвимостях в сформированных подмножествах;

4) определение интенсивности атак на доступность элемента веб-сервера как максимального значения усредненной за год частоты фиксации информации об уязвимостях;

5) определение критичности атаки как средней величины базовой оценки CVSS для уязвимостей выбранного подмножества за год.

В табл. 1 приведен пример подмножества уязвимостей на доступность службы dns за 2003 год (по данным [11]).

Таблица 1

Подмножество уязвимостей доступности службы DNS в период 01.2003 – 12.2003 г.

№п/п	name	published	base_score
1	CVE-2003-0386	2003-07-02	7,5
2	CVE-2003-0432	2003-07-24	10
3	CVE-2003-0636	2003-08-27	7,5
4	CVE-2003-1377	2003-12-31	8,3
5	CVE-2003-1491	2003-12-31	7,5

По данным табл. 1, усредненная заинтересованности уязвимостями доступности dns в 2003 году составила $5{,}7*10^{-4}$ (1/час), а усредненная критичность атак равна 8,16. Эти характеристики являются актуальными и после прошедших десяти лет и, скорее всего, могут рассматриваться как оптимистическая оценка.

Выводы

В статье предложены элементы схемы таксономирования понятий, связанных с атаками на веб-сервисы. На ее основе разработана методика определения интенсивности атак на доступность коммерческого веб-сервера и его элементов.

Дальнейшие исследования следует направить на разработку марковских моделей готовности с учетом атак на уязвимости для разных типов атакующей стороны.

Список литературы

1. Avizienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A.Avizienis, J.-C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.

2. Статистика: Компании по всему миру подвергаются вирусным атакам каждые три минуты [Электронный ресурс]. – Режим доступа к статье: www.securitylab.ru/news/439232.php.

3. Сравнительный анализ моделей систем защиты информации [Электронный ресурс]. – Режим доступа к статье: http://inf-bez.ru/?p=767.

4. Аналитическое исследование по результатам соревнований PHDAYS CTF 2012. Copyright © 2002-2013 Positive Technologies, 2012. – 86 с.

5. The Laws of Vulnerabilities 2.0. [Электронный ресурс]. – Режим доступа: www.qualys.com/research/vulnlaws.

6. Леонов А. Гадание на National Vulnerability Database [Электронный ресурс]. – Режим доступа к статье: securitylab.ru/blog/personal/avleonov/28998.php.

7. 25 Years of Vulnerabilities: 1988-2012 [Электронный ресурс]. – Режим доступа: www.sourcefire.com/25yearsofvulns.

8. Климовский А. Таксономия кибератак и ее применение к задаче формирования сценариев их проведения / А. Климовский // Труды ИСА РАН. – 2006. – Т. 27. – С. 74-107.

9. Бизня А. Организация межсетевого взаимодействия локальных вычислительных сетей, подключение к Интернет, сетевая безопасность / А. Бизня // Публикации трудов семинара «Живые встречи» декабрь 2011 г. [Электронный ресурс]. – Режим доступа к статье: meeting.intertax.ru/static/materials/3/AlexeyBiznya.pdf.

10. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения / Е.С.Вентцель, Л.А.Овчаров. – М.: Высш. школа, 2000. – 383 с.

11. Абдул-Хади А.М. Разработка базовых марковских моделей для исследования готовности коммерческих веб-сервисов / А.М. Абдул-Хади, Ю.Л. Поночовный, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2013. – Вип. 5(64). – С. 186-191.

12 Расширенный поиск по базе уязвимостей [Электронный ресурс]. – Режим доступа к статье: web.nvd.nist.gov/view/vuln/search-advanced.

Поступила в редколлегию 19.06.2013

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ОЦІНКА ИНТЕНСИВНОСТИ АТАК НА ВРАЗЛИВОСТІ ДОСТУПНОСТІ КОМЕРЦІЙНИХ ВЕБ-СЕРВІСІВ

Alaa Mohammed Абдул-Хаді

У статті розглянуті питання оцінки інтенсивності атак на доступність комерційних веб-сервісів і їх елементів. Проведено аналіз осіб, які виконують атаки, їх цілей і мотивів, засобів експлуатації вразливостей. Висунуто гіпотезу про марковість процесів, обумовлених подіями проведення атак на веб-сервіс. Розроблено модель розрахунку інтенсивності атак на веб-сервіс і його елементи, на підставі її визначено інтенсивність і критичність атак на доступність служб dns.

Ключові слова: *інтенсивність атак, уразливості доступності, комерційний веб-сервіс, марківські моделі.*

EVALUATION OF THE ATTACKS RATE ON AVAILABLE VULNERABILITY FOR COMMERCIAL WEB SERVICES

Alaa Mohammed Abdul-Hadi

Assessment technique for the attacks rate on the availability of commercial Web services and service components it's considered in the article. The analysis of the persons performing the attack, their goals and motives, means exploitation of vulnerabilities. The hypothesis of Markov processes for the events of the attacks to the web service is formulated. A model for calculating the attack rate on web services is determined on the basis of its rate and critical attacks on the availability of services dns.

Keywords: *attacks rate, vulnerability on availability, commercial web service, Markov models.*