УДК 681.321

В.С. Харченко, Алаа Мохаммед Абдул-Хади, Ю.Л. Поночовный

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

ФОРМИРОВАНИЕ ПОДМНОЖЕСТВ УЯЗВИМОСТЕЙ ДОСТУПНОСТИ КОММЕРЧЕСКИХ ВЕБ-СЕРВИСОВ

Исследованы вопросы формирования подмножеств – выборок уязвимостей доступности коммерческих веб-сервисов и их элементов. На основе определенных критериев выбран репозитарий уязвимостей и проанализированы его особенности. Проанализирована система оценки уязвимостей CVSS и обоснованы критерии формирования выборки уязвимостей доступности. Рассмотрен практический пример формирования выборок уязвимостей доступности служб DNS и DHCP.

Ключевые слова: *уязвимости доступности, availability, коммерческий веб-сервис, репозитарий, выборка уязвимостей.*

Введение

Успешное развитие современных коммерческих веб-сервисов возможно при условии адекватной оценки кибернетического пространства и принятии обдуманных и своевременных решений, проведении соответствующих мероприятий, направленных на обеспечение их информационной безопасности и надежности. В первую очередь, это касается оценки уязвимостей веб-сервиса как сложной, распределенной клиент-серверной системы. В связи со спецификой коммерческого использования, успешное существование и развитие веб-сервиса возможно только при условии положительного дохода от его эксплуатации. Между тем, расчет окупаемости тесно связан с аналитическими моделями оценки времени работоспособности и простоев системы, комплексно объединенных в модели доступности (availability) [1]. Входными параметрами модели доступности являются интенсивности (вероятностные частоты) некоторых событий, обуславливающих смену состояний системы. В аспекте информационной безопасности, такими событиями являются внешние воздействия (атаки), использующие его уязвимости и нарушающие доступность сервиса.

Начиная с 1999 года, усилиями компании MITRE Corporation (http://www.mitre.org) внедряются независимые от различных производителей стандарты и средства идентификации и учета уязвимостей, атак, конфигураций и др. элементов информационной безопасности [2]. Применительно к уязвимостям, это стандарты CVE (Common Vulnerabilities and Exposures) и CVSS (Common Vulnerability Scoring System).

В разработке CVE помимо экспертов MITRE принимали участие специалисты ISS, Cisco, BindView, Axent, NFR, L-3, CyberSafe, CERT, Carnegie Mellon University, институт SANS, UC Davis Computer Security Lab, CERIAS и т.д. при поддержке компаний Internet Security Systems, Cisco, Axent, BindView, IBM и других. В данной работе используется русскоязычный перевод стандартов и терминов, согласно рекомендациям, введенным в 2012 году МСЕ (ITU-T) серии X-15xx [3, 4, 5].

В идеальном случае (согласно [3]) репозитарий уязвимостей (хранилище данных про известные уязвимости) должен содержать полную характеристику каждой уникальной (по идентификатору CVE) уязвимости согласно системы оценки CVSS (которая, как известно, включает три группы оценок по 6, 3 и 5 показателей в каждой, рис. 1). Однако, только несколько существующих репозитариев (из сорока, отмеченых в [6]) содержат оценки базовой и временной групп. К сожалению, не существует моделей и методов определения интенсивности атак, нарушающих доступность сервиса.

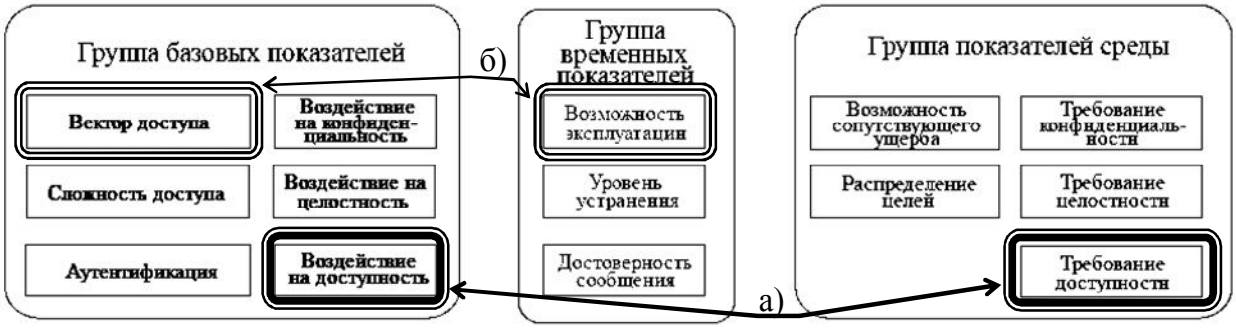

Рис. 1. Группы показателей системы CVSS, в том числе и влияющих на доступность

Далеко не все уязвимости позволяют атакующей стороне нарушить доступность сервиса. Поэтому, в интересах решения задачи определения интенсивности атак на доступность нет смысла обрабатывать всю совокупность данных репозитория. Для решения конкретной задачи необходимо выполнить выборку из системы классификации по требуемым параметрам – определить требуемое подмножество уязвимостей. Так, для решения задачи оценки доступности необходимо выполнить выборку уязвимостей, опасных для доступности заданных элементов системы.

Постановка задачи исследования

В данной статье ставится задача:

– определить репозитарий (базу данных), на основании которого будет формироваться выборка – подмножество уязвимостей, опасных для доступности;

– выделить критерии формирования подмножеств (выборок) уязвимостей для дальнейшего исследования;

– определить методы получения и обработки информации об уязвимостях из выбранного репозитария.

Актуальность проводимых исследований обуславливается высокой динамичностью отрасли и постоянными изменениями и модификациями как стандартов (в скором времени ожидается принятие CVSS v.3), так и инструментариев (репозитарии постоянно пополняются, расширяются и модифицируются).

Выбор репозитария уязвимостей

В данное время активно используется несколько десятков различных репозитариев уязвимостей [6], как правило, представленных в виде интерактивных веб-сервисов. При обосновании выбора репозитария были приняты следующие критерии:

– полнота (емкость, количество уязвимостей);

– доступность данных (бесплатная база);

– удобство получения данных (интерфейсы);

– поддержка оценки уязвимостей по системе CVSS.

На официальном сайте *cve.mitre.org* зарегистрирован 41 репозитарий (ни одного русскоязычного). Наиболее емким и обновляемым считается *nvd.nist.gov*. К его преимуществам, кроме того, относятся:

– наличие встроенных средств поиска и фильтрации данных по базе [7];

– доступность всей базы в интерфейсе XML [8];

– бесплатность доступа к данным.

К недостаткам базы следует отнести наличие только базовой группы оценок, частичное покрытие CWE, ограниченную работоспособность механизма расширенного поиска.

Выбор оценок уязвимостей из системы CVSS

Так как рассматриваются модели доступности, то, в первую очередь, интересны оценки влияния уязвимости на доступность. В явном виде их две (рис.1, а):

– группа «Базовые показатели» – показатель "воздействие на доступность" (Availability impact, A), принимает значения – Отсутствует, (None, N); Частичное, (Partial, P); и Полное, (Complete, C);

– группа «Показатели среды» – показатель «Требование доступности AR», имеет три возможных значения: "низкое" (low), "среднее" (medium) или "высокое" (high).

Также для оценки и выбора множеств уязвимостей важны следующие показатели (рис. 1, б):

– группа «Базовые показатели» – Показатель "вектор доступа" (Access Vector, AV), принимает значения: Локальный, (Local, L); Соседняя сеть, (Adjacent network, A); Сетевой, (Network, N);

– группа «Временные показатели» – Показатель "возможность эксплуатации" (Exploitability, E), принимает значения: Непроверенная, (Unproven, U); Доказана правильность концепции, (Proof-of-Concept, POC); Функциональная, (Functional, F); Высокая, (High, H); Не определено, (Not Defined, ND);

– оценка «Базовая формула» (BaseScore), принимает значение в интервале 0…10 и условно классифицируется на Low (0…4), Medium (4…7) и High (7…10).

Как было отмечено, далеко не все репрозитарии предоставляют информацию по группам «Временные показатели» и «Показатели среды». Между тем, как отмечается в стандарте CVSS, временная оценка не превышает базовую и не более чем на 33% меньше ее; оценка среды, находящаяся в пределах от 0 до 10, не превышает временную оценку. Следовательно, при начальных расчетах можно ограничиться базовыми показателями (рис. 2).

Критерии формирования выборки уязвимостей, опасных для доступности коммерческих веб-сервисов

Учитывая специфику области исследований (коммерческие веб-серверы), были введены следующие ограничения для формирования подмножеств – выборок уязвимостей:

– показатель "вектор доступа" – значение Сетевой, (Network, N);

– показатель "воздействие на доступность" (Availability impact, A), значение – Частичное, (Partial, P);

– показатель "воздействие на доступность" (Availability impact, A), значение – Полное, (Complete, C).

Кроме того, дополнительным условием фильтрации выборки выступает элемент структурной схемы веб-сервера, в котором обнаружена уязвимость, например, DNS-сервер.

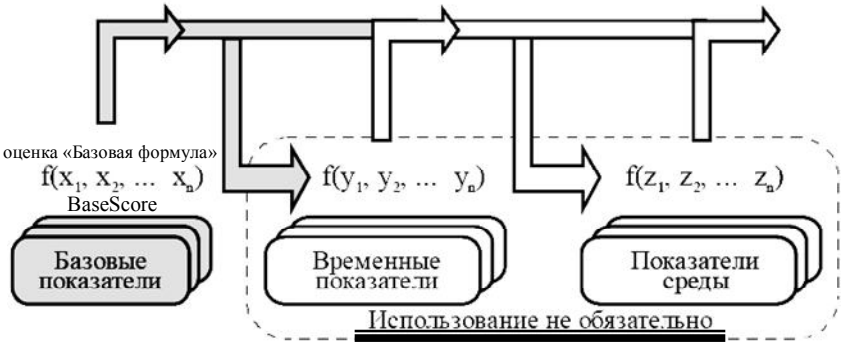

Рис. 2. Последовательность расчета и обязательность оценок CVSS

Инструментарий и последовательность формирования выборки

Для анализа небольшого множества уязвимостей (объем до 50 ед.) можно воспользоваться страницей расширенного поиска по базе [7]. В расширенном поиске по базе nvd.nist.gov данные выдачи разделены на страницы по 20 записей на каждой. Это существенно затрудняет получение и обработку выборки большого объема и делает нецелесообразным ручную обработку данных для решения поставленных задач. Поэтому выбран более приемлемый вариант обработки базы уязвимостей в виде XML – документов. Для этого необходимо скачать с сайта XML за соответствующий год. Для исследования были выбраны данные, которые содержатся в разделе «NVD/CVE XML Feed with CVSS and CPE mappings (version 1.2)».

Документы, полученные с сайта XML, были обработаны с помощью табличного редактора MS Exel. После открытия документа в редакторе в соответствующих столбцах были установлены условия фильтрации:

– CVSS_vector – содержит – AV:N, A:C и A:P;

– ns1:descript – содержит – DNS (пример для изучения атак на dns).

Для полученных в результате фильтрации множеств уязвимостей необходимо зафиксировать параметры «published» и «CVSS_base_score» (табл. 1, 2). Следует отметить, что для формирования подмножества уязвимостей отдельного элемента веб-сервера правильнее было бы проводить выборку не по критерию «содержит» ключевое слово (например, dns); а по соответствию уязвимости заданным идентификаторам CWE [9]. Однако, сейчас репозитарий nvd.nist.gov не обеспечивает покрытие идентификаторов CWE в полном объеме, и не переносит связи уязвимостей с CWE в XML-документы. Поэтому данный метод формирования подмножеств уязвимостей будет применяться после соответствующей модернизации базы NVD.

Таблица 1

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

№п/п	name	published	CVSS_base_score	CVSS_vector
1	CVE-2003-0386	2003-07-02	7,5	(AV:N/AC:L/Au:N/C:P/I:P/A:P)
2	CVE-2003-0432	2003-07-24	10	(AV:N/AC:L/Au:N/C:C/I:C/A:C)
3	CVE-2003-0636	2003-08-27	7,5	(AV:N/AC:L/Au:N/C:P/I:P/A:P)
4	CVE-2003-1377	2003-12-31	8,3	(AV:N/AC:M/Au:N/C:P/I:P/A:C)
5	CVE-2003-1491	2003-12-31	7,5	(AV:N/AC:L/Au:N/C:P/I:P/A:P)

Таблица 2

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

№п/п	name	published	CVSS_base_score	CVSS_vector
1	CVE-2003-0026	2003-01-17	7,5	(AV:N/AC:L/Au:N/C:P/I:P/A:P)
2	CVE-2003-1009	2004-03-29	10	(AV:N/AC:L/Au:N/C:C/I:C/A:C)

Выводы

В статье рассмотрены элементы методики формирования подмножеств уязвимостей доступности коммерческих веб-серверов и их элементов. В качестве источника – репозитария уязвимостей выбрана база nvd.nist.gov. Приведен пример двух выборок – подмножеств уязвимостей доступности служб dns и dhcp. Дальнейшие исследования следует направить на разработку моделей оценивания интенсивности атак на уязвимости, а также исследование влияния входных параметров на результирующие показатели оценки непрерывности функционирования (готовности и доступности) веб-сервисов коммерческого применения.

Список литературы

1. Боярчук А.В. Разработка и исследование базовых моделей отказоустойчивых Web-сервисов / А.В. Боярчук, Ю.Л. Поночовный, В.С. Харченко // Радиоэлектронные и компьютерные системы. – 2010. – № 5(46). – С. 42-49.

2. Уязвимости компьютерных систем и их классификация. [Электронный ресурс]. – Режим доступа к ресурсу: www.in-nov.ru/node/844/

3. Рекомендация МСЭ-Т X.1500. Методы обмена информацией о кибербезопасности. – Женева, 2012. – 36 с.

4. Рекомендация МСЭ-Т X.1520. Общеизвестные уязвимости и незащищенность. – Женева, 2012. – 22 с.

5. Рекомендация МСЭ-Т X.1521. Система оценки общеизвестных уязвимостей. – Женева, 2012. – 32 с.

6. Список лицензированных репозитариев уязвимостей. [Электронный ресурс]. – Режим доступа к ресурсу: http://cve.mitre.org/compatible/vulnerability_management.html.

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

8. Доступ к базе уязвимостей с интерфейсом XML. [Электронный ресурс]. – Режим доступа к ресурсу: nvd.nist.gov/download.cfm#XML.

9. Рекомендация МСЭ-Т X.1524. Перечень общеизвестных слабых мест. – Женева, 2012. – 22 с.

Поступила в редколлегию 19.06.2013

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

ФОРМУВАННЯ ПІДМНОЖИН УРАЗЛИВОСТЕЙ ДОСТУПНОСТІ КОМЕРЦІЙНИХ ВЕБ-СЕРВІСІВ

В.С. Харченко, Алаа Мохаммед Абдул-Хаді, Ю.Л. Поночовний

Досліджено питання формування підмножин вразливостей доступності комерційних веб-сервісів. На основі визначених критеріїв обрано репозитарій вразливостей та розглянуто його особливості. Проаналізовано систему оцінки вразливостей CVSS та обґрунтовано критерії формування вибірки вразливостей доступності. Розглянуто практичний приклад формування вибірок вразливостей доступності служб DNS і DHCP.

Ключові слова: *уразливості доступності, готовність, комерційний веб-сервіс, репозитарій, вибірка вразливостей.*

FORMATION OF AVAILABILITY VULNERABILITY SUBSETS FOR COMMERCIAL WEB-SERVICES

V.S. Kharchenko, Alaa Mohammed Abdul-Hadi, Yu.L. Ponochovny

The paper deals with the formation of subsets of the availability vulnerabilities for commercial web services and their components. On the basis of certain criteria it is selected repository of vulnerabilities and analysed its features. The system of evaluation CVSS vulnerabilities and justified criteria for sampling vulnerability are researched. A practical example of sampling availability vulnerabilities for DNS, and DHCP is described.

Keywords: *vulnerability availability, commercial web service, repository, single vulnerabilities.*