Никита С. Жданов[1], Андрей В. Матерухин[2]
Московский государственный университет геодезии и картографии,
Гороховский пер., 4, Москва, 105064, Россия
[1]e-mail: zhdanow3b@ya.ru, https://orcid.org/0000-0002-3687-6843
[2]e-mail: a_materuhin@miigaik.ru, https://orcid.org/0000-0002-9576-9925

ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНОЙ ЛАБОРАТОРНОЙ СРЕДЫ ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАВЫКАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

DOI: http://dx.doi.org/10.26583/bit.2020.4.08

Аннотация. В статье описывается разработанная авторами виртуальная лабораторная среда для обучения навыкам тестирования на проникновение с обоснованием принятых проектных решений, а также результаты проведенного исследования применимости разработанной виртуальной лабораторной среды для обучения навыкам тестирования на проникновение в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность». Показано, что виртуальная лабораторная среда для обучения навыкам тестирования на проникновение вполне может быть реализована с использованием программного обеспечения с открытым исходным кодом. Реализованная программная среда предъявляет достаточно умеренные требования к аппаратной платформе (конкретизированные в тексте статьи), на которой она должна выполняться. Проведенное исследование применимости показало, что разработанная виртуальная лабораторная среда может быть использована в учебном процессе с применением дистанционных образовательных технологий и позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности.

Ключевые слова: виртуальная лабораторная среда, навыки тестирования на проникновение, информационная безопасность, дистанционное обучение.
Для цитирования: ЖДАНОВ, Никита С.; МАТЕРУХИН, Андрей В. ИСПОЛЬЗОВАНИЕ ВИРТУАЛЬНОЙ ЛАБОРАТОРНОЙ СРЕДЫ ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАВЫКАМ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 95–107, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1309>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.08.

Nikita S. Zhdanov[1], Andrey V. Materukhin[2]
Moscow State University of Geodesy And Cartography,
Gorokhovsky lane, 4, Moscow, 105064, Russia
[1]e-mail: zhdanow3b@ya.ru, https://orcid.org/0000-0002-3687-6843
[2]e-mail: a_materuhin@miigaik.ru, https://orcid.org/0000-0002-9576-9925

Using a virtual laboratory environment for penetration-testing skills training

DOI: http://dx.doi.org/10.26583/bit.2020.4.08

Abstract. This paper describes the virtual laboratory environment developed by the authors for training penetration-testing skills with justification of the design decisions, as well as the results of the study of the applicability of the developed virtual laboratory environment for teaching penetration-testing skills in the educational process of bachelor's degree in information security program. It has been shown that a virtual lab environment for training penetration-testing skills can be implemented using open source software. The implemented software environment makes rather moderate requirements to the hardware platform (specified in the paper) on which it should be executed. The study of applicability has shown that the developed virtual laboratory environment can be used in the educational process of bachelor's degree in information security program with the use of distance learning technologies and allows students to develop practical skills in using penetration testing methods on examples of objects of various levels of complexity.

Keywords: virtual laboratory environment, penetration-testing skills, information security, distance learning.
For citation: ZHDANOV, Nikita S.; MATERUKHIN, Andrey V. Using a virtual laboratory environment for penetration-testing skills training. IT Security (Russia), [S.l.], v. 27, n. 4, p. 95–107, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1309>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.08.

Введение

При проведении аудита информационной безопасности для оценки уровня защищенности компьютерных систем в последние годы все чаще используется тестирование на проникновение. В монографии [1] достаточно убедительно обосновано, что тестирование на проникновение представляет собой один из основных типов аудита критической информационной инфраструктуры. В монографии в частности сказано, что «…тестирование является более гибким инструментом аудита чем, например, мероприятия оценки соответствия, так как его проведение не ограниченно рамками действующих стандартов и регламентов В [2] отмечено, что использование методов обхода систем безопасности сетевых сервисов и проникновения в открытые информационные системы является основным методом проведения аудита безопасности информационных систем. Это мнение, на наш взгляд, излишне радикально, однако оно отражает возрастающую роль методов тестирования на проникновения в проведении оценки уровня защищенности компьютерных систем. Согласно [3], «контроль состояния защищенности относится к категории так называемых превентивных защитных механизмов». Тестирование на проникновение позволяет реализовать главное назначение превентивной защиты – обнаружить уязвимость в защищаемой системе, что позволит обеспечить ее устранение и тем самым предотвратить возможные атаки с ее использованием.

Таким образом, навыки тестирования на проникновения становятся все более востребованы работодателями в области информационной безопасности, что делает формирование этих навыков в процессе обучения в вузе по направлению «Информационная безопасность» актуальной задачей. Однако использование упражнений, направленных на формирование этих навыков, в обычных компьютерных классах, являющихся частью сети университета, может привести к непредвиденным последствиям для этой сети. В [4] термин «тестирование на проникновение» определяется как метод оценки защищенности компьютерной системы или сети, основанный на имитации действий внешнего злоумышленника (не обладающего правами на доступ к системе) или инсайдера (обладающего определенным уровнем доступа)». Согласно [5], «тестирование на проникновение позволяет в достаточно короткие сроки объективно оценить реальный уровень защищенности информационных активов организации в условиях современного состояния способов несанкционированного доступа к информации». Достаточно очевидно, что использование способов несанкционированного доступа к информации в условиях университетской сети может привести как минимум к затруднениям в ее использования другими службами и учебными подразделениями университета. Это связано с тем, что в такого рода упражнениях студенты применяют различные инструменты, которые можно использовать для взлома систем.

Стандартное решение состоит в том, что потенциально опасные инструменты, вовлеченные в процесс обучения, должны использоваться отдельно от потенциально уязвимых систем, чтобы гарантировать, что эти инструменты не вызовут непредвиденных проблем в этих системах. Такой подход означает создание отдельной сети с атакующим и целевым компьютерами, не связанной с общеуниверситетской сетью. Недостатком этого

подхода, помимо дополнительных расходов на настройку и установку полностью изолированной системы, является невозможность корректно использовать ресурсы сети Интернет при выполнении упражнений.

Альтернативой описанному стандартному решению является создание виртуальной лабораторной среды в сети университета. Такая среда, в случае ее надлежащей реализации, может обеспечить защиту для реальных систем университета, позволяя обучаемым выполнить как полный спектр атак, так и провести оборонительные учения с использованием виртуальных машин.

В настоящей статье описывается разработанная авторами виртуальная лабораторная среда для обучения навыкам тестирования на проникновение с обоснованием принятых проектных решений, а также результаты проведенного исследования применимости разработанной виртуальной лабораторной среды для обучения навыкам тестирования на проникновение в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность».

1. Краткий обзор работ по использованию виртуальных лабораторных сред для обучения студентов навыкам тестирования на проникновение

Использование сетевых виртуальных лабораторий в вузах началось довольно давно. Первые обнаруженные нами публикации на русском языке на данную тему относятся еще к концу 90-х годов прошлого века. Это, например, работа [6], которая описывает программные средства для создания виртуальных лабораторий. Следует заметить, что первоначально виртуальные лаборатории рассматривались как некоторый программно-аппаратный комплекс, позволяющий проводить эксперименты в некоторой предметной области без непосредственного контакта с реальной экспериментальной установкой или при полном отсутствии таковой. Важное преимущество такого подхода, как отмечено в [7], заключается в возможности использования виртуальной лаборатории в дистанционном обучении. Позже использование термина «виртуальная лаборатория» расширилось. В [8] виртуальные лаборатории рассматриваются как реализации интерактивных аттестующих элементов с автоматической проверкой ответов, доступ к которым обеспечивается средствами системы дистанционного обучения.

Несмотря на то, что работ, посвященных различным аспектам разработки и использования виртуальных лабораторий довольно много, почти все они не затрагивают предметную область информационной безопасности. Особенно мало академических работ, в которых рассматриваются аспекты разработки и использования виртуальной лабораторной среды для обучения студентов навыкам тестирования на проникновение.

В [9] описывается разработка и применение лабораторных стендов на основе платформ виртуализации для получения специалистами навыков и знаний о сетевой инфраструктуре объекта перед проведением реального аудита информационной безопасности. В работе обоснованы ограничения существующих готовых лабораторных стендов и средств для их построения в контексте обучения аудиту информационной безопасности, а также описывается разработанная виртуальная лаборатория. Это довольно интересное с нашей точки зрения решение, но оно слишком специализировано и предназначено для использования специалистами, уже обладающими довольно высоким уровнем подготовки, а поэтому не подходит для использования в условиях подготовки бакалавров информационной безопасности.

В [10] описана специализированная виртуальная лаборатория, позволяющая производить настройку и проверку DLP-системы, определять политику безопасности, обеспечивать контроль информационных потоков в компании, а также анализировать

выявленные инциденты. Решение основано на применении программного обеспечения компании InfoWatch, хорошо показывает возможности использования виртуализации в учебном процессе, но также является узкоспециализированным и не может рассматриваться как основа для формирования – навыков тестирования на проникновение.

В [11] приводится разработка Национального исследовательского университета «МИЭТ» – учебно-методический комплекс по подготовке к аудиту информационной безопасности магистрантов по направлению подготовки 10.04.01 «Информационная безопасность» по программе – «Аудит информационной безопасности автоматизированных систем», а также программный комплекс для построения среды виртуализации для моделирования сетевой инфраструктуры на базе симуляторов сетей Netsimulator, IMINES, Core, Mininet. Недостатком такого решения, с нашей точки зрения, является применение проприетарного программного обеспечения, что делает затруднительным настройку виртуальной среды под потребности обучения навыкам тестирования на проникновение.

В [12] при анализе необходимых характеристик лабораторной среды для тестирования на проникновения указано, что основной характеристикой должна быть ее универсальность, позволяющая исследовать различные типы атак. При создании виртуальной лаборатории, по мнению авторов работы [12], следует учитывать ограниченную мощность персонального компьютера (ПК), которая должна позволять проводить тестирование на проникновение. В качестве уязвимой информационной системы используется Metasploitable. По мнению авторов работы [12], уникальность их решения заключается в быстроте, доступности и легкости развертывания по сравнению с более сложными лабораториями, для функционирования которых необходимо более одного ПК. Разработанная ими лабораторная среда поддерживает стабильную работу на среднем по мощности ПК. Это объясняется тем, что основными компонентами являются Unix-подобные операционные системы на базе ядра Linux, обладающие сравнительно небольшими системными требованиями. Благодаря этому качеству лаборатория может быть развернута на ноутбуках и в компьютерных классах для обучения.

В [13] авторы также используют Metasploitable в качестве платформы для обучения студентов эксплуатации уязвимостей. Авторы отмечают, что практически каждый открытый сетевой порт является точкой входа в систему, а преимуществом Metasploitable является высокая удобность и эффективность.

Однако с нашей точки зрения работы [12–13] не позволяют создать на основе описываемых ими решений учебную платформу для студентов, поскольку использование в качестве уязвимой цели Metasploitable, в которой все возможные уязвимости одновременно доступны для возможного использования, затрудняет процесс обучения и контроля правильности выполнения учебных заданий.

В [14] авторы рассматривают возможность использования заданий из популярного ресурса root-me.org в качестве дополнения для разработанных ими лабораторных работ. На ресурсе root-me.org проводятся соревнования по информационной безопасности в формате «Захват флага» (CTF, Capture The Flag)[1]. Ресурс поддерживает английский, немецкий, французский и испанский языки, имеет большую базу уязвимостей, отсортированных по направлениям. Название заданий описывает уязвимость, эксплуатация которой позволит решить задание. Присутствует ранговая система начисления баллов за решенное задание: чем сложнее задание, тем больше за него начисляют баллов. По нашему мнению, ресурс действительно можно использовать в

[1]Root Me: Hacking and Information Security learning platform. URL: https://www.root-me.org (accessed: 10.10.2020).

качестве дополнительного материала в обучении в вузе, но для этого необходимо провести довольно большую предварительную методическую работу.

Ближе всего к нашему представлению о возможной реализации виртуальной лабораторной среды для обучения студентов методам тестирования на проникновения находятся решения, описанные в [15–18], в которых описывается использование в качестве платформы облачного кластера Гродненского государственного университета. Согласно [15], эта платформа используется с 2012 г., реализована на основе OpenNebula, а в качестве системы виртуализации использует Kernel-based Virtual Machine (KVM). В кластере реализовано три учебных лаборатории – начального, среднего и высокого уровня сложности. Работа обучаемого в лабораторной среде осуществляется на основе методики «серый ящик»: перед началом исследования предоставляется информация об инфраструктуре в виде схемы и описания деятельности виртуальной компании. Для автоматизации проверки ответов на задания лабораторий используются уникальные для каждого обучаемого токены (флаги), отмечающие соответствие найденной в результате проникновения уязвимости, требуемым эталонам. Прохождение начального уровня сложности открывает доступ к прохождению среднего уровня сложности, а затем высокого.

В работе [18] авторы выделяют три основных вектора составления заданий, соответствующие уровням сложности:

– сетевая безопасность (начальный уровень сложности);
– безопасность веб-приложений (средний уровень сложности);
– обнаружение атак (высокий уровень сложности).

Очень интересным, с нашей точки зрения, является решение, использованное для создания виртуальной лабораторной среды в Эдинбургском университет имени Нейпира (Edinburgh Napier University), описанное в [19]. В этой работе описано использование двух облачных сред – одна имитировала большой набор серверов и компьютеров обычных пользователей в самых разных сетевых конфигурациях, а другая имитировала набор компьютеров с установленными на них операционными системами семейства Linux с разными незакрытыми известными уязвимостями.

К сожалению, при всей привлекательности решений для создания виртуальной лабораторной среды в [15–19] они не могут быть использованы в нашем университете вследствие недостаточности материально-технической базы для ее реализации. Как нам представляется, это не только проблема нашего университета – в аналогичной ситуации находятся и многие другие российские университеты, реализующие программы по направлению «Информационная безопасность». Поэтому нами была разработана и реализована виртуальная лабораторная среда для обучения навыкам тестирования на проникновение, которая основана на использовании программного обеспечения с открытым исходным кодом и которая не требует наличия в университете дорогостоящего вычислительного кластера.

2. Требования к функционалу виртуальной лабораторной среды

В результате проведенного предварительного анализа были определены следующие обязательные требования к функционалу виртуальной лабораторной среды:

– виртуальная лабораторная среда должна поддерживать выполнение заданий, связанных с тестированием сетевой безопасности;

– виртуальная лабораторная среда должна иметь средства автоматизации проверки правильности выполнения задания;

– задания должны быть разделены по направлениям, соответствующим темам лекционного материала;

– виртуальная лабораторная среда должна обеспечивать разные уровни сложности выполнения заданий и упражнений, при этом начальный уровень сложности должен обеспечить пологость кривой обучаемости.

Использованные инструментальные средства для реализации виртуальной лабораторной среды можно условно разделить на три группы.

В первую группу входят программные средства, реализующие среду реализации. Важно отметить, что поскольку одним из выделенных требований к разрабатываемой среде является сравнительно низкий начальный уровень сложности заданий (кривая обучаемости должна быть пологой), то разумно использовать популярные среды реализации, то есть те, которые обучаемые скорее всего уже знают.

Самой популярной операционной системой для серверов являются системы на базе ядра Linux, поэтому большинство студентов по направлению «Информационная безопасность» уже имеют навыки работы в этой операционной системе. Серверные версии Linux к тому же, полностью соответствуют требованиям по быстроте, доступности и экономичности для системы. Поэтому было решено использовать операционную систему Linux для всех серверов лабораторной среды и среду VirtualBox для виртуализации.

Для реализации многих заданий, связанных с тестированием сетевой безопасности, необходимо использовать веб-сервер. Нами было принято решение использовать программное обеспечение с открытым исходным кодом – веб-сервер Apache. Это один из наиболее популярных веб-серверов[2]. Преимущества Apache в его гибкости, мощности и широкой распространенности. Он хорошо документирован и может быть расширен с помощью системы загружаемых библиотек. Использование этого программного обеспечения позволяет исполнять программы на большом количестве языков программирования без использования внешнего программного обеспечения.

Для хранения учетных данных и результатов обучаемых, было принято решение использовать также программное обеспечение с открытым исходным кодом – систему управления базами данных (СУБД) MySQL. К достоинствам MySQL можно отнести простоту использования, распространенность, а также популярность использования этой СУБД для обучения навыкам работы с базами данных.

Использование PHP в качестве языка веб-разработки обусловлено его популярностью, а также некоторым рядом достоинств:

– PHP специально разработан для веб-разработок и его код может внедряться непосредственно в HTML;

– пользователь не видит исходного PHP кода страницы;

– язык предоставляет широкие возможности программирования и позволяет подключать дополнительные модули и библиотеки;

– язык PHP без подключенных библиотек и модулей уязвим и, вместо создания уязвимостей, достаточно лишь не применять рекомендации по безопасности при разработке веб-приложения.

– связка PHP+MySQL является распространенной связкой для обучения разработке веб-приложений.

Для автоматизации проверки ответов на задания решено было использовать утилиту ncat – форк стандартной сетевой утилиты netcat. Данная утилита позволяет

[2]Usage statistics of web servers. URL: https://w3techs.com/technologies/overview/web_server (accessed: 10.10.2020)

общаться системам в одной сети посредством открытия сетевого порта на прослушивание или передачу информации. Использование ncat обусловлено дополнительными опциями, обеспечивающими защиту данных. Опция allow позволяет подключаться к операционной системе только с разрешенного ip адреса, а опция ssl шифрует соединение, исключая возможность перехвата данных.

Во вторую группу инструментальных средств для реализации виртуальной лабораторной среды входят программные средства для реализации уязвимостей в тестовой лабораторной среде. Классификацией векторов атак и уязвимостей занимается сообщество Open Web Application Security Project (OWASP).

Согласно списку OWASP TOP-10 2017 г. самыми распространенными векторами атак на веб-приложения являются:

1. Внедрение кода.
2. Некорректная аутентификация.
3. Незащищенность конфиденциальных данных.
4. Внедрение внешних XML-сущностей.
5. Нарушение контроля доступа.
6. Небезопасная конфигурация.
7. Межсайтовый скриптинг.
8. Небезопасная десериализация.
9. Использование компонентов с известными уязвимостями.
10. Недостаточное логирование и мониторинг.

Не все из представленных векторов атак представляют интерес для реализации в лабораторной среде. Наш выбор уязвимостей для реализации был основан на том, что задания на их основе должны быть простыми и понятными студенту, который только начал знакомиться с техниками тестирования на проникновение.

Нами были отобраны следующие вектора атак:

– внедрение кода и в качестве реализации данного вектора атаки – использование sql-инъекций в запросы к СУБД MySQL;

– некорректная аутентификация, представленная в виде cookie с именем пользователя;

– нарушение контроля доступа – отсутствие дополнительных проверок доступа к административной панели, кроме пароля;

– небезопасная конфигурация и в качестве реализации данного вектора атаки – простые пароли служб и аккаунтов, а также загрузка исполняемых файлов с PHP кодом из административной панели веб-приложения;

– использование компонентов с известными уязвимостями – уязвимое программное обеспечение FTP службы; уязвимость в команде sudo, позволяющая непривилегированным пользователям запускать команды с правами суперпользователя (уязвимость CVE-2019-14287[3]).

К третьей группе инструментальных средств для реализации виртуальной лабораторной среды относятся программные приложения, при помощи которых можно выявлять и эксплуатировать уязвимости. К этой группе утилиты для работы с возможными уязвимостями. Для нашей виртуальной лабораторной среды мы не стали ограничивать обучаемых в выборе этих средств, ограничившись рекомендацией использовать Kali Linux или любой другой популярный дистрибутив для тестирования на проникновение. В

[3]Potential bypass of Runas user restrictions. URL: https://www.sudo.ws/alerts/minus_1_uid.html (accessed: 10.10.2020)

процессе выполнения заданий студенты пользовались такими утилитами как Nmap, Hashcat, Hydra, BurpSuite, Metasploit Framework.

3. Описание разработанной виртуальной лабораторной среды

Общая структура разработанной тестовой лабораторной среды приведена на рис. 1.

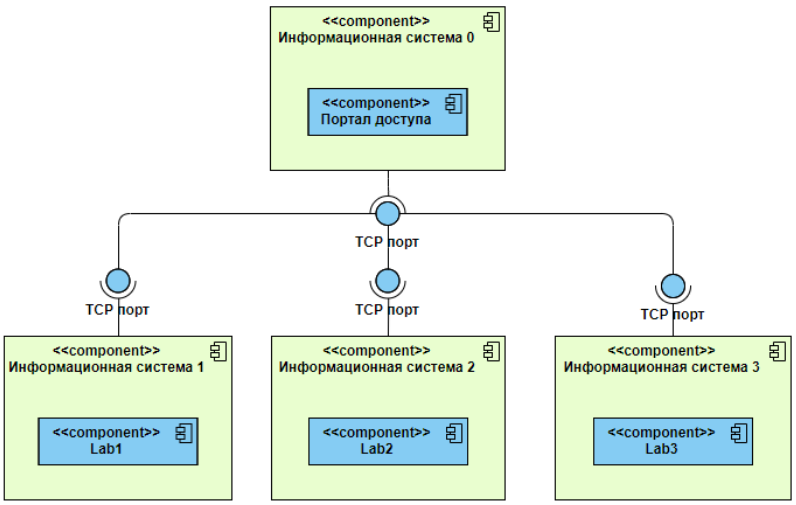

Рис. 1. UML диаграмма структуры тестовой лабораторной среды
(Fig. 1. UML diagram of the test laboratory structure)

Тестовая лабораторная среда состоит из:

– информационной системы с учебным сайтом, на котором расположены учетные записи студентов, задания, рейтинговая таблица;

– информационной системы с установленными уязвимыми компонентами (Lab1, Lab2 и Lab3 соответствующие лабораторным работам);

– канала связи между ними.

В состав тестовой лабораторной среды входят четыре виртуальные машины с установленными ОС Linux Ubuntu 18.04 LTS Server, а также установлен Apache веб-сервер и СУБД MySQL, проведены специальные настройки и установки.

Виртуальная лабораторная среда для обучения навыкам тестирования на проникновение содержит лабораторные работы, соответствующие трем направлениям:

1. Эксплуатация уязвимостей веб-приложения.
2. Эксплуатация уязвимостей сервера.
3. Применение полученных навыков.

Для реализации методики «серый ящик» в названии каждого задания помещена подсказка, позволяющая студенту понять эксплуатация уязвимости какого вида приведет к решению этого задания.

Задания и уязвимости соответствуют темам лекционного материала.

Необходимо было разработать и реализовать такой алгоритм, который отвечает следующим требованиям:

1. Ответ для каждого студента уникален.
2. Поддерживается работа нескольких студентов над одним заданием.
3. Передача данных должна осуществляться по зашифрованному каналу связи.

Решено было использовать утилиту ncat с дополнительными опциями allow для разрешения доступа к каналу связи только порталу доступа и ssl для шифрования

передаваемых данных. Алгоритм валидации ответа был реализован при помощи bash скриптов и php кода внутри страницы задания.

Портал доступа к тестовой лабораторной среде предполагает авторизацию студента для доступа к заданию. Авторизация происходит при помощи подключенного к странице php скрипта, обращающегося к СУБД MySQL, где хранятся учетные данные пользователей и таблица заданий. Авторизовавшись, студент получает доступ к заданиям. Было принято решение не нагружать систему дополнительными программными средствами и ограничиться применением стандартного элемента HTML – фрейма. Использование HTML фреймов обусловлено такими факторами, как удобство использования и возможность динамического расширения контента учебного сайта. На рис. 2 представлен итоговый вид портала доступа после прохождения процедуры авторизации.

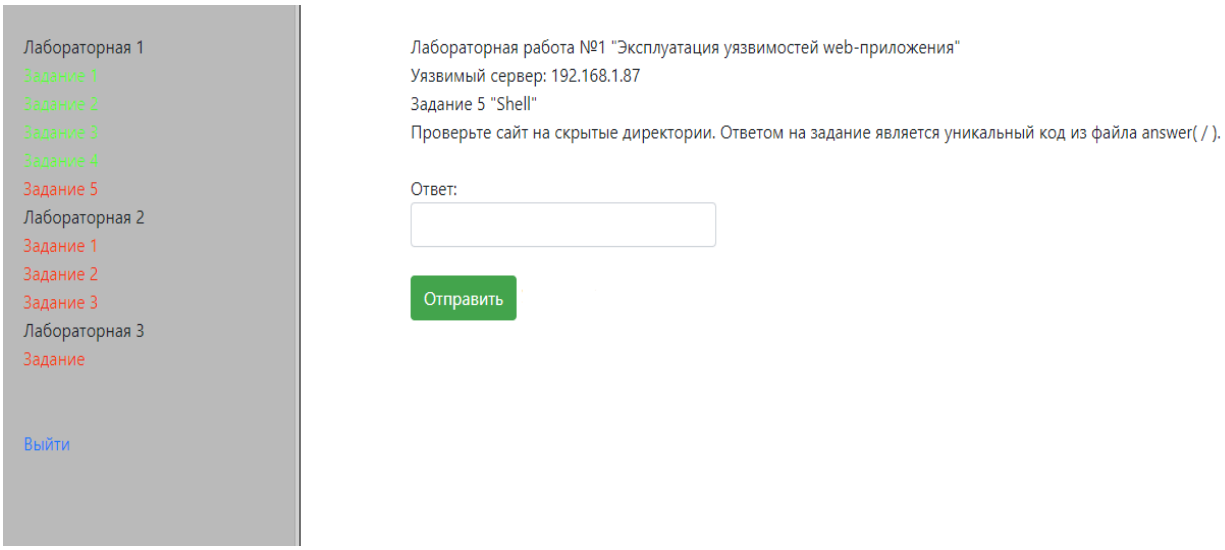

Рис. 2. Общий вид портала доступа
(Fig. 2. General view of the access portal)

Из рис. 2 видно, что страница разделена на 2 основных фрейма – фрейм задания и фрейм меню. В задании есть строчка с указанием адреса уязвимого приложения, а также поле ввода ответа и кнопка проверки ответа.

В меню выполненные задания обозначены зеленым цветом, а не выполненные – красным.

Унификация веб-приложений уязвимых информационных систем и портала доступа к заданиям позволила использовать одинаковые программные конструкции, что позволит упростить планируемое в дальнейшем расширение списка выполняемых лабораторных работ.

4. Исследование применимости и дальнейшее направление развития

Для исследования применимости разработанной виртуальной лабораторной среды для обучения навыкам тестирования на проникновение в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность» программное обеспечение виртуальной лабораторной среды было установлено на аппаратную платформу в следующей конфигурации: 2 процессора Intel Xeon CPU E5-2690, 2.90GHz, 256Gb RAM. С привлечением студентов третьего и четвертого курсов были проверены различные варианты подключения к виртуальной лабораторной среде (из сети

университета, из дома, с использованием различных устройств), а также проведено нагрузочное тестирование с целью определить предельное значение количества одновременно комфортно работающих (то есть без возникновения субъективного чувства «торможения» системы) в виртуальной среде студентов. Исследование показало, что, по крайней мере, 30 студентов в условиях дистанционного обучения могут комфортно работать в системе на использованной аппаратной платформе.

Другим вопросом, на который должно было ответить исследование, был вопрос о том, действительно ли использование разработанной виртуальной среды позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение. Разработанная виртуальная лабораторная среда для тестирования на проникновение была использована для проведения лабораторных работ в течение весеннего семестра 2020 г. по дисциплине «Программно-аппаратные средства защиты информации. В исследовании принимало участие 24 студента (1 группа). Заданием для проверки навыков была выбрана третья лабораторная работа, охватывающая весь спектр уязвимостей, представленных ранее.

Результаты начального тестирования выявили неспособность студентов самостоятельно решить это задание (рис. 3). Итоговое тестирование, проведенное в конце семестра после выполнения в дистанционном режиме лабораторных работ в виртуальной лабораторной среде, показало, что более чем у 80 % студентов, прошедших обучение, были сформированы устойчивые практические навыки использования методов тестирования на проникновение (рис. 4).

Полученные результаты, по нашему мнению, показывают, что использование виртуальной лабораторной среды в учебном процессе по направлению подготовки 10.03.01 «Информационная безопасность» действительно позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности

Планируемое дальнейшее развитие разработанной виртуальной лабораторной среды связано с тем, что Московский государственный университет геодезии и картографии (МИИГАиК) является признанным российским центром компетенций как в области обработки геопространственных данных, так и в области обеспечения защиты таких данных.

Рис. 3. Диаграмма начального тестирования (Fig. 3. Diagram of primary testing)

Рис. 4. Диаграмма итогового тестирования (Fig. 4. Diagram of final testing)

В работе [20] уже было указано, что все более широкое распространение как геоинформационных систем, так и систем сбора и обработки пространственных данных, сделало обеспечение безопасности в этой специфической сфере одним из весьма востребованных приложений технологий информационной безопасности. При разработке политики безопасности для геоинформационных систем необходимо учитывать характеристики геопространственных данных, а также то, что набор возможных уязвимостей для геоинформационных систем или систем сбора пространственно-временных данных обладает особенностями, характерными именно для этого типа компьютерных систем.

Заключение

В работе показано, что виртуальная лабораторная среда для обучения навыкам тестирования на проникновение вполне может быть реализована с использованием программного обеспечения с открытым исходным кодом. Реализованная программная среда предъявляет достаточно умеренные требования к аппаратной платформе, на которой она должна выполняться. Проведенное исследование применимости разработанной виртуальной лабораторной среды в условиях дистанционного обучения показало, что для поддержки одновременной работы 30 студентов в этой виртуальной среде вполне достаточно мини-кластера в следующей конфигурации: 2 процессора Intel Xeon CPU E5-2690, 2.90GHz, 256Gb RAM. Исследование также показало, что использование виртуальной лабораторной среды в учебном процессе действительно позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности.

Дальнейшим направлением развития виртуальной лабораторной среды в университете МИИГАиК является разработка тестовых виртуальных машин с установленными на них различными типами геоинформационных систем или систем сбора пространственно-временных данных.

СПИСОК ЛИТЕРАТУРЫ:

1. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. СПб.: Наукоемкие технологии, 2018. – 122 с. URL: https://elibrary.ru/item.asp?id=36445362 (дата обращения: 10.10.2020).
2. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. – 272 с. ISBN 978-5-4461-0662-2.
3. Горбатов, Виктор С.; Мещеряков, Алексей А. Сравнительный анализ средств контроля защищенности вычислительной сети. Безопасность информационных технологий, [S.l.]. Т. 20. № 1. С. 43–48, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/354 (дата обращения: 10.10.2020).
4. Котляров В.П. Современный подход к анализу уязвимостей информационных систем / В.П. Котляров, К.А. Ядыменко // Путь науки. 2014. Т. 1, № 9 (9). С. 38–41. URL: https://elibrary.ru/item.asp?id=22509935 (дата обращения: 10.10.2020).
5. Чуб, В. С. Аудит безопасности информационной системы с использованием тестов на проникновение // Молодой исследователь Дона. 2018. № 6 (15). С. 88–90. URL: https://elibrary.ru/item.asp?id=36903527 (дата обращения: 10.10.2020).
6. Дмитриев В.М., Зайченко Т.Н., Шутенков А.В Универсальная моделирующая среда для создания виртуальных лабораторий //В сборнике: Технический университет: дистанционное инженерное образование. Труды Международной научно-практической конференции. Министерство общего и профессионального образования РФ, Ассоциация технических университетов, Томский политехнический университет. 1998. С. 194–195.
7. Трухин А.В. Об использовании виртуальных лабораторий в образовании // Открытое и дистанционное образование. 2002. № 4 (8). С. 81–82. URL: https://elibrary.ru/item.asp?id=14794890 (дата обращения: 10.10.2020).
8. Вашенков О.Е., Волкова А.А., Лямин А.В. Примеры реализации сетевых виртуальных лабораторий в среде системы дистанционного обучения //Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2007. № 45. С. 157–163. URL: https://elibrary.ru/item.asp?id=11543701 (дата обращения: 10.10.2020).

9. Иванов А.А., Настинов Э.О. Разработка виртуальной лаборатории для моделирования сетевой инфраструктуры объекта аудита //В сборнике: Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-2019. Доклады Всероссийской конференции (с международным участием). Сер. "Научные конференции, посвященные дню Радио" 2019. С. 279–283. URL: https://elibrary.ru/item.asp?id=39137554 (дата обращения: 10.10.2020).
10. Калиберда Е.А., Шабалин А.М Использование современных систем виртуализации для формирования профессиональных компетенций студентов вузов при изучении DLP-систем // Наука о человеке: гуманитарные исследования. 2020. Т. 14. № 2. С. 118–122. URL: https://elibrary.ru/item.asp?id=43811417 (дата обращения: 10.10.2020).
11. Воеводин В.А. Учебно-методический комплекс по подготовке к аудиту информационной безопасности //В сборнике: ПРЕПОДАВАТЕЛЬ ГОДА 2019 сборник статей первого тура Международного научно-методического конкурса. 2019. С. 273–283. URL: https://elibrary.ru/item.asp?id=39132731 (дата обращения: 10.10.2020).
12. Красов А.В. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем / А.В. Красов, С.И. Штеренберг, А.И. Москальчук // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38–46. URL: https://elibrary.ru/item.asp?id=42576548 (дата обращения: 10.10.2020).
13. Стефінко Я. Я. Використання FOSS на платформі KALI Linux та Metasploitable для вивчення процесу етичного хакінгу / Стефінко Я. Я., Піскозуб А. З. // FOSS Lviv 2014, 24-27 квітня 2014 року: – Л.:, 2014. С. 118–121. URL: http://elartu.tntu.edu.ua/handle/123456789/16912 (дата обращения: 10.10.2020).
14. Кобилев, М.А. Опыт создания интерактивной образовательной платформы на основе инструментария соревнований ctf / М.А. Кобилев, Д.С. Зеленский, Е.С. Абрамов // Информационное противодействие угрозам терроризма. 2015. № 24. С. 321–328. URL: https://elibrary.ru/item.asp?id=23603864 (дата обращения: 10.10.2020).
15. Кадан А.М. Облачные лаборатории для задач тестирования на проникновение / А.М. Кадан, А.К. Доронин // Современные информационные технологии и ИТ-образование. 2016. Т. 12. № 3-1. С. 104–110. URL: https://elibrary.ru/item.asp?id=27411981 (дата обращения: 10.10.2020).
16. Кадан А.М. Виртуальные облачные лаборатории в подготовке специалистов направления "Компьютерная безопасность" / А.М. Кадан, С.А. Зайкова // Информатизация образования. 2015. № 2. С. 37–43. URL: https://elibrary.ru/item.asp?id=32844265 (дата обращения: 10.10.2020).
17. Кадан А.М. Облачный кластер университета в подготовке студентов направления "Компьютерная безопасность" // Ученые записки института социальных и гуманитарных знаний. Вып. 1(13): материалы VII международной научн.-практ. конф. "Электронная Казань 2015". Казань: ЮНИВЕРСУМ, 2015. С. 245–250. URL: https://elib.grsu.by/doc/13890 (дата обращения: 10.10.2020).
18. Кадан А.М. Изучение методов тестирования на проникновение в подготовке специалистов по защите информации / А.М. Кадан, А.К. Доронин // Информатизация образования. 2016. № 2. С. 3–11. URL: https://elibrary.ru/item.asp?id=32844238 (дата обращения: 10.10.2020).
19. Buchanan, William & Ramsay, Bruce & Macfarlane, Richard & Smales, Adrian & Russell, Gordon & (Jr, Bill. (2015). Teaching Penetration Testing and Malware Analysis within a Cloud-based Environment. URL:https://www.researchgate.net/publication/281030350_Teaching_Penetration_Testing_and_Malware_Analysis_within_a_Cloud-based_Environment (дата обращения: 10.10.2020).
20. Матерухин А.В. Особенности реализации образовательной программы по направлению подготовки 10.03.01 Информационная безопасность в Московском государственном университете геодезии и картографии с учетом специфики вуза // В сборнике: Актуальные проблемы обеспечения информационной безопасности. Труды Межвузовской научно-практической конференции. 2017. С. 146–150. URL: https://elibrary.ru/item.asp?id=29725564 (дата обращения: 10.10.2020).

REFERENCES:

[1] Makarenko S.I. Audit bezopasnosti kriticheskoj infrastruktury` special`ny`mi informacionny`mi vozdejstviyami. Monografiya. SPb.: Naukoemkie texnologii, 2018. – 122 s. URL: https://elibrary.ru/item.asp?id=36445362 (accessed: 10.10.2020) (in Russian).
[2] Skabczov N. Audit bezopasnosti informacionny`x sistem. SPb.: Piter, 2018. – 272 s. ISBN 978-5-4461-0662-2 (in Russian).
[3] Gorbatov, Victor S.; Meshcheryakov, Aleksey A. Comparative Analysis of Computer Network Security Scanners. IT Security (Russia), [S.l.]. Vol. 20. no. 1. P. 43–48, 2013. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/354 (accessed: 10.10.2020) (in Russian).
[4] Kotlyarov V.P., Yadymenko K.A. Modern approach to the analysis of information system vulnerability. Put` nauki. 2014. T. 1. № 9 (9). P. 38–41. URL: https://elibrary.ru/item.asp?id=22509935 (accessed: 10.10.2020) (in Russian).

[5] Chub, V. S Information system safety audit using penetration testing. Molodoj issledovatel` Dona. 2018. № 6 (15). P. 88–90. URL: https://elibrary.ru/item.asp?id=36903527 (accessed: 10.10.2020) (in Russian).
[6] Dmitriev V.M., Zajchenko T.N., Shutenkov A.V Universal`naya modeliruyushhaya sreda dlya sozdaniya virtual`ny`x laboratorij. V sbornike: Texnicheskij universitet: distancionnoe inzhenernoe obrazovanie. Trudy` Mezhdunarodnoj nauchno-prakticheskoj konferencii. Ministerstvo obshhego i professional`nogo obrazovaniya RF, Associaciya texnicheskix universitetov, Tomskij politexnicheskij universitet. 1998. S. 194–195 (in Russian).
[7] Truxin A.V. Ob ispol`zovanii virtual`ny`x laboratorij v obrazovanii. Otkry`toe i distancionnoe obrazovanie. 2002. № 4 (8). S. 81–82. URL: https://elibrary.ru/item.asp?id=14794890 (accessed: 10.10.2020) (in Russian).
[8] Vashenkov O.E., Volkova A.A., Lyamin A.V. Primery` realizacii setevy`x virtual`ny`x laboratorij v srede sistemy` distancionnogo obucheniya. Nauchno-texnicheskij vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta informacionny`x texnologij, mexaniki i optiki. 2007. № 45. S. 157–163. URL: https://elibrary.ru/item.asp?id=11543701 (accessed: 10.10.2020) (in Russian).
[9] Ivanov A.A., Nastinov E`.O. Development of a virtual laboratory for modeling network infrastructure of audit object. V sbornike: Radioe`lektronny`e ustrojstva i sistemy` dlya infokommunikacionny`x texnologij - RE`US-2019. Doklady` Vserossijskoj konferencii (s mezhdunarodny`m uchastiem). Ser. "Nauchny`e konferencii, posvyashhenny`e dnyu Radio" 2019. S. 279–283. URL: https://elibrary.ru/item.asp?id=39137554 (accessed: 10.10.2020) (in Russian).
[10] Kaliberda E.A., Shabalin A.M The impact of modern virtualization systems on university students' professional competences while studying dlp systems. Nauka o cheloveke: gumanitarny`e issledovaniya. 2020. T. 14. № 2. P. 118–122. URL: https://elibrary.ru/item.asp?id=43811417 (accessed: 10.10.2020) (in Russian).
[11] Voevodin V.A. Uchebno-metodicheskij kompleks po podgotovke k auditu informacionnoj bezopasnosti. V sbornike: PREPODAVATEL` GODA 2019 sbornik statej pervogo tura Mezhdunarodnogo nauchno-metodicheskogo konkursa. 2019. S. 273–283. URL: https://elibrary.ru/item.asp?id=39132731 (accessed: 10.10.2020) (in Russian).
[12] Krasov A.V., Shterenberg S.I., Moskal`chuk A.I. Virtual laboratory creation for distributed information system safety testing. Vestnik Bryanskogo gosudarstvennogo texnicheskogo universiteta. 2020. № 3 (88). S. 38–46. URL: https://elibrary.ru/item.asp?id=42576548 (accessed: 10.10.2020) (in Russian).
[13] Stefinko Ya. Ya., Piskozub A. Z. Using FOSS on the platform KALI Linux and Metasploitable for the study of the Ethical Hacking. FOSS Lviv 2014 (Lviv, 24-27 April 2014). P. 118–121. URL: http://elartu.tntu.edu.ua/handle/123456789/16912 (accessed: 10.10.2020) (in Ukrainian).
[14] Kobilev, M.A., Zelenskij D.S., Abramov E.S. Xperience in working with interactive educational platform based on ctf competition tools. Informacionnoe protivodejstvie ugrozam terrorizma. 2015. № 24. P. 321–328. URL: https://elibrary.ru/item.asp?id=23603864 (accessed: 10.10.2020) (in Russian).
[15] Kadan A.M., Doronin A.K. Oblachny`e laboratorii dlya zadach testirovaniya na proniknovenie. Sovremenny`e informacionny`e texnologii i IT-obrazovanie. 2016. T. 12. № 3-1. S. 104–110. URL: https://elibrary.ru/item.asp?id=27411981 (accessed: 10.10.2020) (in Russian).
[16] Kadan A.M., Zajkova S.A Virtual cloud laboratories in training of specialists of the direction "computer security". Informatizaciya obrazovaniya. 2015. № 2. S. 37–43. URL: https://elibrary.ru/item.asp?id=32844265 (accessed: 10.10.2020) (in Russian).
[17] Kadan A.M. University cloud cluster in the training of students of computer security direction. Ucheny`e zapiski instituta social`ny`x i gumanitarny`x znanij. Vy`p. 1(13): materialy` VII mezhdunarodnoj nauchn.-prakt. konf. "E`lektronnaya Kazan` 2015". – Kazan`: YuNIVERSUM, 2015. S. 245–250. URL: https://elib.grsu.by/doc/13890 (accessed: 10.10.2020) (in Russian).
[18] Kadan A.M., Doronin A.K. The study of methods for penetration testing in training of information security specialists. Informatizaciya obrazovaniya. 2016. № 2. P. 3–11.URL https://elibrary.ru/item.asp?id=32844238 (accessed: 10.10.2020) (in Russian).
[19] Buchanan, William & Ramsay, Bruce & Macfarlane, Richard & Smales, Adrian & Russell, Gordon & (Jr, Bill. (2015). Teaching Penetration Testing and Malware Analysis within a Cloud-based Environment. URL:https://www.researchgate.net/publication/281030350_Teaching_Penetration_Testing_and_Malware_Analysis_within_a_Cloud-based_Environment (accessed: 10.10.2020).
[20] Materuxin A.V. Osobennosti realizacii obrazovatel`noj programmy` po napravleniyu podgotovki 10.03.01 informacionnaya bezopasnost` v Moskovskom gosudarstvennom universitete geodezii i kartografii s uchetom specifiki vuza. V sbornike: Aktual`ny`e problemy` obespecheniya informacionnoj bezopasnosti. Trudy` Mezhvuzovskoj nauchno-prakticheskoj konferencii. 2017. S. 146–150. URL: https://elibrary.ru/item.asp?id=29725564 (accessed: 10.10.2020) (in Russian).

Поступила в редакцию – 10 октября 2020 г. Окончательный вариант – 06 ноября 2020 г.
Received – October 10, 2020. The final version – November 06, 2020.