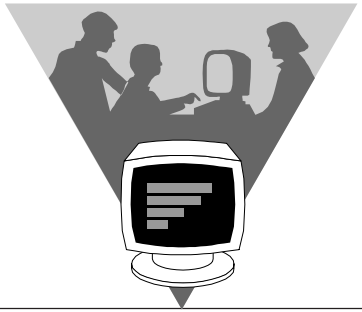



***А.М. Кадан**, к.т.н., доцент, заведующий кафедрой системного программирования и компьютерной безопасности УО «Гродненский государственный университет имени Янки Купалы»,*
***А.К. Доронин**, стажер-преподаватель кафедры системного программирования и компьютерной безопасности УО «Гродненский государственный университет имени Янки Купалы»*

# Изучение методов тестирования на проникновение в подготовке специалистов по защите информации

Безальтернативное масштабное проникновение информационных технологий во все сферы жизни общества, проходящее без должного внимания к вопросам обеспечения безопасности информации, может принимать драматический характер, что подтверждает поток публикаций в средствах массовой информации и специальных изданиях. Неправомерное разглашение или уничтожение информации, ее компрометация или фальсификация, возможности дезорганизации процессов в современных информационных системах и автоматизированных производствах могут приводить, и уже приводят, к нанесению серьезных материальных потерь и ущерба репутации не только отдельным личностям, но и организациям и государствам.

В ряде вузов республики, в том числе в Гродненском государственном университете им. Я. Купалы, на протяжении ряда лет ведется успешная подготовка специалистов по защите компьютерной информации, хотя, на наш взгляд, потенциал специалистов данного направления в нашей стране востребован не в полной мере. В то же время, в связи с лавинообразным появлением все новых угроз и ростом масштаба их проявлений, существенной проблемой процесса практической подготовки специалистов по защите компьютерной информации становится недостаточная оснащенность программно-технической базы учебных заведений.

Перспективным выходом из этой ситуации как при обучении студентов, так и в рамках переподготовки специалистов, представляется создание и использование современных инфраструктурных решений для создания виртуальных лабораторий, использующих возможности облачных и кластерных архитектур.

## Преступления в сфере информационных технологий или киберпреступность

Общественная опасность противоправных действий в области информационных технологий связана с тем, что такие действия могут вступить в противоречие с положениями Закона РБ «Об информации, информатизации и защите информации» [1] в отношении личных данных и конфиденциальной информации. А также могут повлечь нарушение деятельности автоматизированных систем управления и контроля различных объектов, нарушение работы компьютерных систем; несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов; иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным, но и с физическим ущербом.

Согласно УК РБ [2] преступлениями против информационной безопасности (глава 31 УК РБ) являются: несанкционированный доступ к компьютерной информации (ст. 349 УК РБ); модификация компьютерной информации (ст. 250 УК РБ); компьютерный саботаж (ст. 251 УК РБ); неправомерное завладение компьютерной информацией (ст. 252 УК РБ); изготовление либо сбыт специальных средств для получения

неправомерного доступа к компьютерной системе или сети (ст. 253 УК РБ); разработка, использование либо распространение вредоносных программ (ст. 254 УК РБ); нарушение правил эксплуатации компьютерной системы или сети (ст. 255 УК РБ).

Зачастую совершение преступлений в сфере компьютерной информации сопряжено с совершением иных уголовно наказуемых деяний, в частности, таких как нарушение тайны переписки (ст. 203 УК РБ), нарушение авторских, смежных, изобретательских и патентных прав (ст. 201 УК РБ), кража (ст. 205 УК РБ), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 216 УК РБ), мошенничество (ст. 209 УК РБ), вымогательство (ст. 208 УК РБ) и пр.

Методы оказания противодействия указанным противоправным действиям, многие из которых связаны с проблемами несанкционированного проникновения злоумышленника в инфраструктуру информационных систем, входят в круг задач подготовки специалистов по защите информации.

## Киберпреступления и задачи тестирования на проникновение

Основные виды киберпреступлений (преступлений в сфере информационных технологий, связанных с незаконными действиями людей, использующих информационные технологии для преступных целей) связаны с несанкционированным использованием различных технических устройств и систем удаленного доступа; созданием и распространением вредоносного кода, взломом паролей, кражей реквизитов банковских карт; а также с распространением противоправной информации (клевета, материалы для разжигания межнациональной и межрелигиозной розни и т.п.) через информационно-коммуникационные сети [3].

Для снижения уровня опасности реализации киберпреступлений популярной во всем мире услугой в области информационной безопасности становится тестирование на проникновение. Суть его заключается в санкционированной попытке аудитора обойти существующий комплекс средств защиты информационной системы. В ходе тестирования на проникновение аудитор играет роль злоумышленника, мотиви-

рованного на нарушение информационной безопасности сети заказчика.

Тестирование на проникновение (сокращение от англ. – penetration testing, на сленге «пентест») – это поиск уязвимостей с практической проверкой возможностей их реализации. Цель тестирования на проникновение – оценка уровня защищенности, которая заключается в исследовании сети или веб-ресурса для выявления уязвимостей, которые могут быть использованы злоумышленником для реализации угроз информационной безопасности [4].

Очевидными достоинствами методов тестирования на проникновение являются: высокая достоверность сведений о выявленных уязвимостях благодаря фактическому подтверждению возможности их использования злоумышленником; достаточность результатов исследования для оценки критичности выявленных уязвимостей; наглядность получаемых результатов.

К недостаткам методов тестирования на проникновение можно отнести: способность исследователя воспроизводить только действия нарушителя, равного ему или уступающего по квалификации, и, как следствие, – высокие требования к квалификации исследователя и невысокая достоверность сведений об отсутствии уязвимостей; низкую степень автоматизации действий исследователя, и, как следствие, – высокие затраты по сравнению с другими способами оценки уровня защищенности.

Очевидно, что подготовка таких специалистов, способных проводить тестирование на проникновение по заказу организаций, предполагает не только наличие теоретических знаний, но и использование специализированных лабораторий со специально сконфигурированной инфраструктурой и программно-технической базой.

## Выбор платформы для создания учебных лабораторий

В учебном процессе кафедры системного программирования и компьютерной безопасности ГрГУ им. Я. Купалы в качестве платформы для обучения методам исследования информационных систем на проникновение выбран облачный кластер Гродненского государственного университета. Кластер используется в университете с 2014 года, работает на

платформе OpenSource-продукта OpenNebula, в качестве системы виртуализации использует KVM.

Выбор кластера для создания лабораторий обусловлен возможностью формирования профильных библиотек образов вычислительных машин (ВМ) с комплектами программного обеспечения (ПО) учебного назначения; возможностью быстрого пакетного развертывания, обновления, удаления однотипных виртуальных рабочих мест или лабораторий целиком; формированием (на основе набора ВМ) лабораторных макетов распределенных систем; возможностью подключения виртуальных машин к локальной сети университета.

Использование платформы OpenNebula также позволило реализовать ряд возможностей, необходимых для обучения методам защиты информации: тестирование в облаке антивирусного ПО без вероятности повреждения оборудования студентов; развертывание ВМ с различными уязвимыми сетевыми сервисами, используемыми для обучения сканированию безопасности сети; развертывание фермы ВМ Linux и Windows для изучения отдельных уязвимостей операционных систем; развертывание виртуальных машин для обучения технологиям защиты от утечек информации (использование DLP-систем, программных комплексов для анализа угроз и уязвимостей, систем защиты сетей и рабочих станций), связанных с обеспечением управления информационной безопасностью организаций.

Возможности облачного кластера на базе OpenNebula позволяют эффективно использовать его также для организации соревнований по практической защите компьютерной информации различного формата и уровня. Например, существующая инфраструктура OpenNebula была выбрана в качестве базы при проведении очного тура по защите информации в рамках Республиканской олимпиады по криптографии и защите информации 2015, 2016 годов.

В то же время нельзя не отметить и некоторые недостатки использования облачного кластера для обучения методам тестирования на проникновение: подготовка мастер-образов и шаблонов ВМ является весьма трудоемким процессом, требующим не только владения предметной областью, но и навыками системного администрирования Windows и Linux, а также знания особенностей облачной платформы; невозможность использования некоторых ОС семейства

Windows (в частности, Windows XP SP3 и некоторых других, более старых версий) из-за несовместимости с используемым средством виртуализации KVM; требование наличия постоянного подключения к сети Интернет. Очевидно, что при обрыве соединения сеанс связи с облачной платформой будет прекращен. Продолжить работу можно будет только после восстановления подключения к Интернет.

## Использование учебных лабораторий

В рамках развития концепции использования виртуальных лабораторий для задач тестирования на проникновение развернуты три учебных лаборатории: начального, среднего и высокого уровня сложности.

Работа обучаемого в лабораториях осуществляется на основе методики «серый ящик»: перед началом исследования предоставляется информация об инфраструктуре в виде схемы и описания деятельности виртуальной компании. Далее участникам будет предложено выполнить эксплуатацию различных уязвимостей, связанных с работой сетевых и веб-компонентов, криптографических механизмов, с ошибками конфигурации и кода, а также с человеческим фактором.

Каждая из трех лабораторий соответствует определенному уровню сложности («наименьшая», «средняя», «высокая»). Прохождение 1-го уровня открывает доступ к прохождению 2-го, и т.д. Полное прохождение третьего (последнего) уровня потребует от участника наивысших знаний и умений.

Система виртуальных облачных лабораторий интегрирована в образовательную онлайн-платформу университета для того, чтобы обеспечить обучаемым удобный доступ к необходимой теоретической информации.

Для автоматизации проверки результатов проведенного тестирования на проникновение, соответствия найденных токенов (флагов), отмечающих найденную в результате проникновения уязвимость, в локальной сети университета сети развернута система Facebook CTF [5, 6].

Использование платформы Facebook CTF как интерфейса управления процессом тестирования на проникновение позволило активизировать учебный процесс, придав решению задач на проникновение соревновательный характер и эмоциональную окраску.

## Пример облачной лаборатории для тестирования на проникновение

На рис. 1 представлена примерная схема лаборатории среднего уровня сложности.

Далее даны примеры возможных заданий для обучаемых.

1. *Сетевая безопасность*. Описание задачи: Необходимо исследовать сервер, найти все открытые порты, определить сервис и найти токен. Участвующие машины: 172.16.2.1.

2. *Безопасность web-приложений*. Описание задачи: Необходимо исследовать web-приложение, найти уязвимость и проэксплуатировать ее. Найти необходимый токен можно будет после завершения эксплуатации приложения. (Получение токена также открывает доступ к задачам уровня №3). Участвующие машины: 172.16.2.2.

3. *Обнаружение атак*. Легенда. Машина бухгалтерии компании находится под управлением Linux по адресу 172.16.2.11. Также имеется машина Windows по адресу 172.16.2.12, с которой работают те же пользователи.

3.1 *Аудит безопасности 1 (Linux)*. Описание задачи: На Linux-машине определить, какой из уволенных сотрудников ответственен за утечку данных. Участвующие машины: 172.16.2.11 (Linux) – user: *labuser*, password: *labuser.*

3.2 *Аудит безопасности 2 (Linux)*. Описание задачи: Определить, кто из пользователей пытался получить права пользователя root? Участвующие машины: 172.16.2.11 (linux) – user: *labuser*, password: *labuser.*

3.3. *Аудит безопасности 3 (Windows)*. Описание задачи: На Windows-машине найти пользователя, который удалил файл ImportantFile.txt. Участвующие машины: 172.16.2.12 (windows) – user: *John*(AdministratorUser), password: *john.*

3.4. Аудит безопасности 4 (Windows). Описание задачи: Определеить, кто последний получал доступ к файлу ImportantFile.txt перед его удалением (исключая удалившего файл пользователя)? Участвующие машины: 172.16.2.12 (windows) – user: *john*(AdministratorUser), password: *john.*

## Заключение

Использование облачных лабораторий для задач тестирования на проникновение демонстрирует адекватность по-

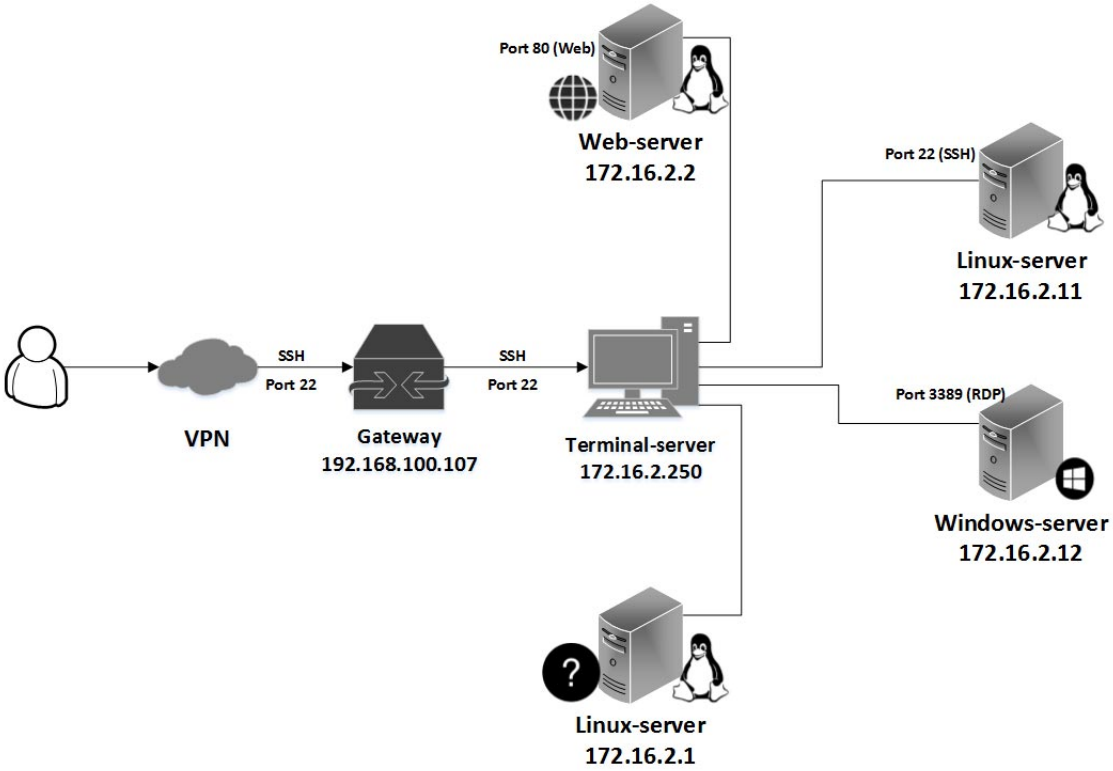


Рис.1. Примерная схема лаборатории среднего уровня сложности

ставленной цели – формированию и совершенствованию навыков обучаемых по тестированию сетевой инфраструктуры на проникновение извне. Основная сложность, с которой пришлось столкнуться разработчикам, это подготовка множества поэтапных заданий и инфраструктуры для их выполнения.

Опыт работы показал, что организация виртуальных облачных лабораторий для тестирования на проникновение является перспективным направлением в организации учебного процесса; может рассматриваться как содержательная квинтэссенция знаний различных учебных дисциплин; является одним из немногих действительно эффективных способов подготовки специалистов с практическими навыками в области защиты информации.

## Литература


1. Об информации, информатизации и защите информации: Закон Республики Беларусь от 10 ноября 2008 г. № 455-З // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2016. – Дата доступа: 16.09.2016

2. Уголовный кодекс Республики Беларусь: с изменениями и дополнениями от 5 января 2016 г. – Изд.: НЦПИ РБ. – 2016. – 320 с.

3. Киберпреступность [Электронный ресурс] / SecurityLab.ru – информационный портал по безопасности. – М.: Positive Technologies. – Режим доступа: http://www.securitylab.ru/news/tags/Киберпреступность/. – Дата доступа: 27.03.2016.

4. Тестирование на проникновение [Электронный ресурс] / Портал по информационной безопасности. ООО «ПентестИТ», 2016. – Режим доступа: https://www.pentestit.ru/audit/penetration-testing. – Дата доступа: 27.03.2016.

5. Facebook выложил на Гитхаб свою платформу для проведения CTF [Электронный ресурс] / Сообщество IT-специалистов. ООО «Хабр», 2016. – Режим доступа: https://habrahabr.ru/post/283380/. – Дата доступа: 27.03.2016.

6. Страница проекта Facebook CTF [Электронный ресурс] / Сайт GitHub. – Режим доступа: https://github.com/facebook/fbctf. – Дата доступа: 27.03.2016.


*Статья поступила 04.11.2016*