УДК 004.01

ВИРТУАЛЬНЫЕ ОБЛАЧНЫЕ ЛАБОРАТОРИИ ДЛЯ ЗАДАЧ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

А.М. Кадан, А.К. Доронин

Рассматриваются вопросы, связанные с созданием современной учебной инфраструктуры на базе облачного кластера для подготовки специалистов в области защиты информации и компьютерной безопасности. Облачный кластер Гродненского государственного университета использует платформу OpenNebula и предлагает современные решения для моделирования инфраструктурных решений, обеспечивающих решение ряда задач информационной безопасности, в частности, задач тестирования на проникновение.

Существенной проблемой процесса обучения практическим мерам защиты компьютерной информации является недостаточная мощность программно-технической базы учебных заведений. Выходом из этой ситуации представляется создание и использование в учебном процессе современных инфраструктурных решений, виртуальных лабораторий, возможностей облачных и кластерных архитектур.

Преступления в сфере информационных технологий

Преступления в сфере информационных технологий или киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют преступления, связанные с использованием мобильных устройств, различных гаджетов и систем дистанционного банковского обслуживания; создание и распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов(скриминг, фишинг); а также распространение противоправной информации (клевета, материалы для разжигания межнациональной и межрелигиозной розни и т.п.) через информационно-коммуникационные сети [1].

Для снижения уровня опасности реализации киберперступлений, популярной во всем мире услугой в области информационной безопасности является тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест). Суть их заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования аудитор играет роль злоумышленника, мотивированного на нарушение информационной безопасности сети заказчика.

Очевидно, что подготовка специалистов, способных проводить тестирование на проникновение по заказу организаций, является процессом, требующим не только наличия теоретических знаний, но и использования специализированной лабораторной программно-технической и инфраструктурной базы.

Тест на проникновение: основные понятия, цели и задачи

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 выявление уязвимостей, которые могут быть использованы злоумышленником для реализации угроз информационной безопасности [2].

Очевидными достоинствами методов тестирования на проникновение являются:

- высокая достоверность сведений о выявленных уязвимостях за счет фактического подтверждения возможности их использования злоумышленниками;
- достаточность результатов исследования для оценки критичности выявленных уязвимостей;
- наглядность получаемых результатов.

К недостаткам методов тестирования на проникновение можно отнеси:

- способность исследователя воспроизводить только действия нарушителя, равного или уступающего по квалификации, и, как следствие, — высокие требования к квалификации исследователя и низкая достоверность сведений об отсутствии уязвимостей;
- низкую степень автоматизации действий исследователя, и, как следствие, — высокие трудозатраты по сравнению с другими способами оценки защищенности.

Преступления в сфере информационных технологий или киберпреступность

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут нарушить требования Закона РБ «Об информации, информатизации и защите информации» [3] в отношении личных данных и конфиденциальной информации, а также повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьёзное 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 ущербом, но и с физическим вредом людям.

По УК РБ [4] преступлениями против информационной безопасности (глава 31 УК РБ) являются:

- *Несанкционированный доступ к компьютерной информации (ст. 349 УК РБ).* Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Сюда относятся взлом веб-ресурса, подмена главной страницы сайта, подбор паролей, взлом БД, проникновение в сеть компании и т.п.

Для привлечения лица к уголовной ответственности недостаточно лишь одного факта совершения им неправомерного доступа к охраняемой законом компьютерной информации. Уголовно наказуемы лишь те деяния, которые повлекли материальные последствия в виде: уничтожения и/или блокирования, модификации, копирования компьютерной информации.

- *Модификация компьютерной информации (ст. 250 УК РБ).* Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации).

- *Компьютерный саботаж (ст.251 УК РБ).* Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя.

- *Неправомерное завладение компьютерной информацией (ст. 252 УК РБ).* Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда.

- *Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 253 УК РБ).* Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети.

- *Разработка, использование либо распространение вредоносных программ (ст. 254 УК РБ).* Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами. Под данную категорию подпадают троянские кони, бекдоры, шеллкоды, руткиты, ботнеты, черви, вирусы, эксплоиты и т.п; DOS- и DDOS-атаки.

- *Нарушение правил эксплуатации компьютерной системы или сети (ст. 255 УК РБ).* Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда.

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.

- Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 203. ГЛАВА 23. Преступления против конституционных прав и свобод человека и гражданина). Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

- Хищение путем использования компьютерной техники (ст. 211, Глава 24. Преступления против собственности). Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации.

- Причинение имущественного ущерба без признаков хищения (ст. 216. Глава 24. Преступления против собственности). Причинение ущерба в значительном размере посредством извлечения имущественных выгод в результате обмана, злоупотребления доверием или путем модификации компьютерной информации при отсутствии признаков хищения.

- Коммерческий шпионаж (ст. 254. Глава 24. Преступления против собственности). Похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну, с целью их разглашения либо незаконного использования.

Наказание нарушителя зависит от таких факторов как:

- причинение крупного ущерба или совершение преступления из корыстной заинтересованности;
- действие было совершенно группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения;
- наступление тяжких последствий или создание угрозы их наступления.

В Республике Беларусь борьбой с преступлениями в сфере информационных технологий занимается Управление «К» МВД РБ.

Возможности облачного кластера на платформе OpenNebula

В качестве программной основы для облачной инфраструктуры, используемой в учебном процессе, в ГрГУ им. Я. Купалы выбрана платформа OpenNebula. Это свободно распространяемый продукт с открытым исходным кодом, то есть полностью открытая платформа. Она базируется на вычислительных ресурсах программно-аппаратного комплекса на основе оборудования IBM. В качестве системы виртуализации используется KVM.

К преимуществам использования платформы OpenNebula при подготовке ИТ-специалистов и специалистов по защите информации можно отнести:

- Возможность формирования профильных библиотек образов ВМ с комплектами ПО учебного назначения;

- Возможность быстрого пакетного развертывания, обновления, удаления однотипных виртуальных рабочих мест (лабораторий);
- Формирование на основе набора ВМ лабораторных макетов распределенных систем;
- Возможность подключения виртуальных машин к локальной сети ГрГУ им. Я. Купалы через соединение типа «сетевой мост».

Использование платформы OpenNebula позволяет реализовать ряд возможностей для обучения методам защиты информации:

- Тестирование в облаке антивирусного ПО без вероятности повреждения оборудования студентов;
- Развёртывание виртуальной машины с различными уязвимыми сетевыми сервисами, используемой для обучения сканированию безопасности сети;
- Развертывание фермы виртуальных машин Linux и Windows для изучения отдельных тем дисциплины «Операционные системы»;
- Развёртывание виртуальных машин для обучения технологиям защиты от утечек информации (обучение использованию DLP-систем, программных комплексов по анализу угроз и уязвимостей, систем защиты рабочих станций от утечек информации) в рамках дисциплины «Управление информационной безопасностью».

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

Учебная лаборатория для тестирования на проникновение

На данный момент для развёртывания в облачном кластере разрабатывается учебная лаборатория, целью которой является оттачивание навыков тестирования сети на проникновение извне. Работа в лаборатории 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, ошибками конфигурации и кода, а также с человеческим фактором. На рисунке 1 ниже представлена актуальная схема проекта.

На каждом из узлов присутствует уязвимость. В случае успешной эксплуатации всех уязвимостей, участник объявляется победителем. Планируется организовать доступ к лаборатории через VPN-подключение и таким образом сделать её доступной для всех пользователей в сети Интернет.

Отметим, что на схеме присутствует маршрутизатор Cisco. Однако конфигурация платформы OpenNebula не позволяет напрямую эмулировать работу сетевых устройств (маршрутизаторы, коммутаторы и пр.). Для этого

необходимо использовать специальное ПО на отдельной виртуальной машине под управлением Linux. Таким образом, реальная схема сети будет содержать ещё один узел, осуществляющий виртуализацию всех сетевых устройств.

На момент подготовки данного материала в облаке развёрнута и подготовлена к использованию виртуальная машина «Metasploitable Linux», доступная всем пользователям из внутренней сети ГрГУ им. Я. Купалы. Данная машина предназначена для обучения методам эксплуатации наиболее распространённых уязвимостей сетевых служб.

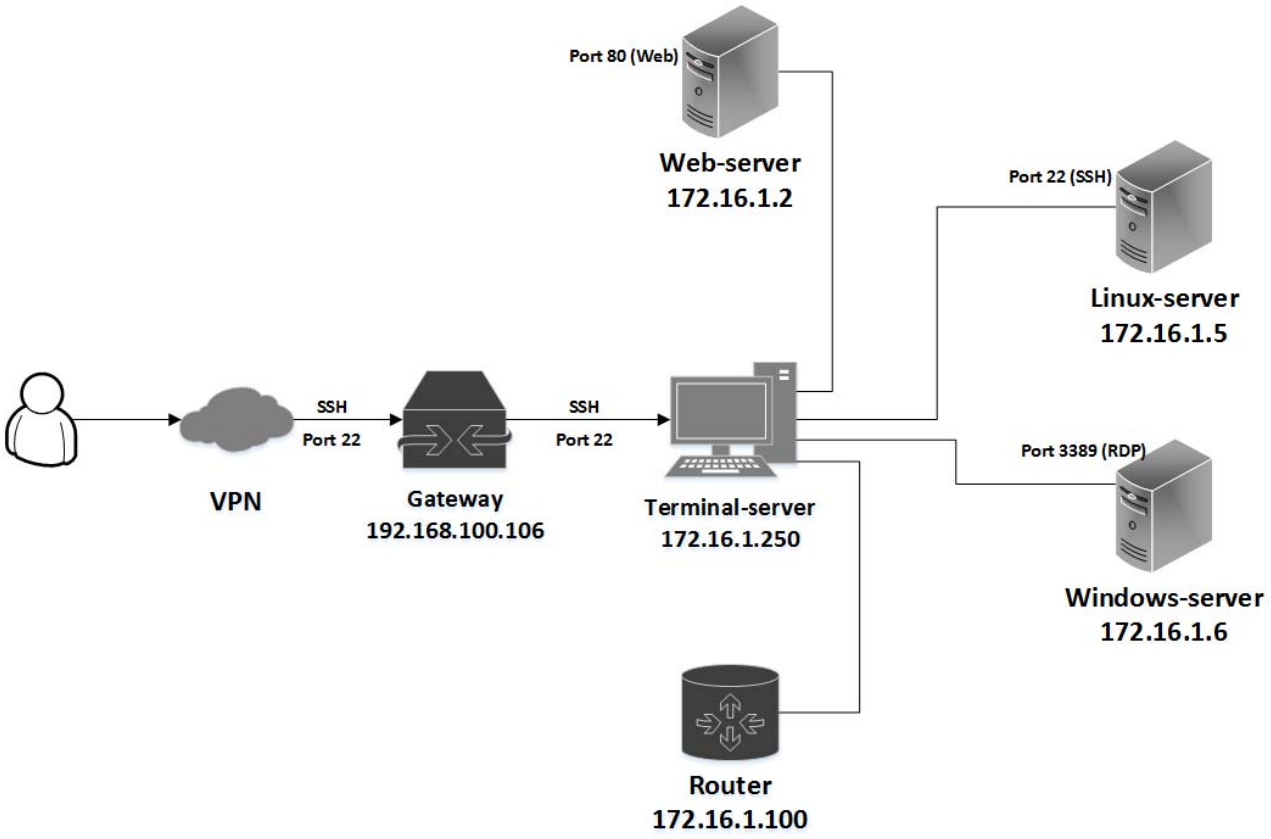

Рисунок 1 – Актуальная схема проекта

Сложности использования учебной лаборатории

Нельзя не отметить и некоторые недостатки использования облачных технологий в учебном процессе:

1. Подготовка мастер-образов и шаблонов ВМ является весьма трудоемким процессом, требующим не только владения предметной областью, но и навыков системного администрирования Windows и Linux, а также знания особенностей облачной платформы.
2. 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.
3. 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.

Список литературы

1. 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.
2. 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.
3. Закон Республики Беларусь “Об информации, информатизации и защите информации” (10 ноября 2008 г. № 455-З) [Электронный ресурс] / Национальный центр правовой информации Республики Беларусь, 2003-2016. - Режим доступа: https http://www.pravo.by/main.aspx?guid=3871&p2=2/1552. – Дата доступа: 27.03.2016.
4. Уголовный кодекс Республики Беларусь [Электронный ресурс] / Национальный центр правовой информации Республики Беларусь, 2006-2016. – Режим доступа: http://etalonline.by/?type=text&regnum=HK9900275#load_text_none_1_. – Дата доступа: 27.03.2016.

Кадан Александр Михайлович, заведующий кафедрой системного программирования и компьютерной безопасности УО «Гродненский государственный университет имени Янки Купалы», кандидат технических наук, доцент

Доронин Алексей Константинович, стажер-преподаватель кафедры системного программирования и компьютерной безопасности УО «Гродненский государственный университет имени Янки Купалы»