А. М. Калинина, Д. С. Смирнов, Т. И. Паюсова
Тюменский государственный университет, г. Тюмень
УДК 004.056

РАЗРАБОТКА И ПОСТРОЕНИЕ ВИРТУАЛЬНОГО СТЕНДА ДЛЯ ПРОВЕДЕНИЯ ЛАБОРАТОРНЫХ ПРАКТИКУМОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В статье представлен разработанный виртуальный стенд, имитирующий инфраструктуру некой организации. Рассмотрены актуальные атаки на инфраструктуру организации и способы защиты от них. На основе изученных атак создана серия лабораторных работ по тестированию на проникновение в информационную инфраструктуру.*
Ключевые слова: *виртуальная лаборатория, безопасность инфраструктуры, пентестинг, тестирование на проникновение, Windows, Active Directory, Kerberos, Golden Ticket.*

Введение. Лаборатории для проведения тестов на проникновение [1] полностью или частично имитируют ИТ-инфраструктуру реальных компаний и создаются для легального взлома и улучшения навыков пентеста. Такие лаборатории позволяют опробовать современные уязвимости [2], изучить новые векторы атак и способы защиты инфраструктуры [3].

Актуальность работы заключается в необходимости обучения будущих специалистов по информационной безопасности возможным векторам атак на инфраструктуру организаций и способам защиты от этих атак. Наличие виртуальной лаборатории позволит вузам использовать ее в учебном процессе. Для проведения лабораторных практикумов студентам не нужно устанавливать на свои компьютеры ресурсоемкие виртуальные машины, так как они развернуты на выделенном серверном оборудовании с необходимыми мощностями, а для получения доступа к лаборатории нужен только интернет, что позволяет проводить семинары в дистанционном формате и быть более гибким при выборе аудитории для проведения очных занятий. Студентам, как будущим специалистам в сфере информационной безопасности, необходимо знать об актуальных атаках, как они устроены, на основе каких уязвимостей и как от них защититься.

Проблема исследования обусловлена необходимостью обучения новых специалистов по информационной безопасности современным методам защиты ИТ-инфраструктуры и формированию более глубокого понимания принципов действия злоумышленников при взломе.

Целью данной работы является создание лабораторного практикума на основе виртуального стенда для проведения тестов на проникновение в инфраструктуру организации для отработки навыков по защите инфраструктуры.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1) изучить существующие виртуальные лаборатории, которые используются для проведения тестов на проникновение;

2) описать вымышленную организацию, инфраструктуру которой будем реализовывать на нашем стенде;

3) рассмотреть и описать уязвимости, которые можно будет использовать в рамках нашего стенда;

4) создать сетевую топологию инфраструктуры;

5) создать и настроить виртуальные машины. Развернуть описанную инфраструктуру в виртуальной лаборатории;

6) внести в виртуальную лабораторию «умышленные» уязвимости;

7) описать варианты защиты от внесенных уязвимостей;

8) создать практические задания на проникновение и защиту инфраструктуры на основе созданного виртуального стенда;

9) произвести апробацию созданного стенда.

Материалы и методы. Для создания виртуального стенда были проанализированы существующие подобные решения, такие как Hack The Box, платформа, представляющая собой как отдельные виртуальные машины, так и целые виртуальные леса Active Directory с различными заданиями, и Лаборатории “Test Lab” от компании Pentestit. В своей работе мы решили использовать существующие механики построения виртуальных лабораторий, т. к. многие лаборатории являются платными иностранными разработками, а наличие собственного виртуального стенда на базе университета позволит

контролировать учебный процесс со стороны преподавателя, так как собственную виртуальную лабораторию можно конфигурировать по своему усмотрению в любое время.

По легенде у нас имеется некая организация, инфраструктуру которой мы реализовали в стенде. Компания занимается разработкой антивирусного программного обеспечения для различных устройств. У компании есть штат разработчиков и тестировщиков, создающих код и тестирующих итоговый продукт.

Для практической части ЦИТ ТюмГУ по запросу предоставил нам выделенный физический сервер. Сервер имеет 144 Гб оперативной памяти, жесткий диск на 500 Гб и 2 процессора Intel Xeon по 6 ядер. Подключение к серверу происходит с помощью VPN университета по RDP.

На рис. 1 представлена сетевая инфраструктура виртуальной лаборатории, которая максимально приближена к реальной организации, в ней имеется главный офис и филиал, соединенные vpn подключением. В главном офисе находится контроллер домена и вебсервер, в филиале резервный контроллер домена, развернуто несколько служб и приложений.

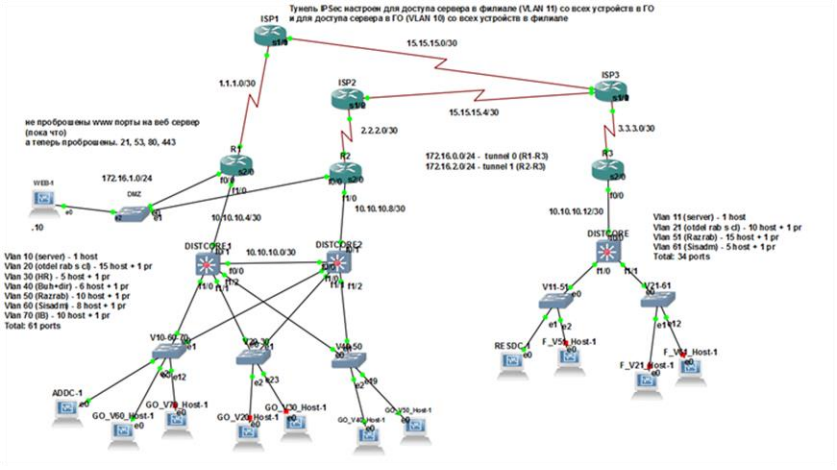


Рис. 1. Сетевая инфраструктура виртуальной лаборатории

При создании стенда были сконфигурированы все серверы и рабочие станции инфраструктуры в соответствии с общими рекомендациями по информационной безопасности. Были настроены парольные политики, разграничение прав доступа с помощью Active Directory, подразумевается, что каждый отдел имеет доступ только в необходимую ему часть инфраструктуры. Для проведения же атак необходимо, чтобы выполнялись определенные условия, иначе реализовать атаку, разумеется, не получится. В конфигурацию нашей системы мы внесли соответствующие изменения, чтобы было возможным проведение атак, описанных в лабораторных заданиях.

Изучив известные актуальные атаки, направленные на хищение данных и повышение привилегий в Windows системах, были внесены соответствующие уязвимости в систему: были добавлены уязвимости на веб-сервер, чтобы можно было произвести атаки с использованием инъекций. Для того чтобы можно было выполнить лабораторные работы, были созданы учетные записи с различными правами доступа в Active Directory и была проведена имитация работы пользователей для того, чтобы в локальных базах данных хостовых машин сохранилась информация об учетных записях.

На основе исследованных атак были изучены способы защиты от них.

В лабораторных работах описаны практические рекомендации по устранению уязвимостей и противодействию атакам.

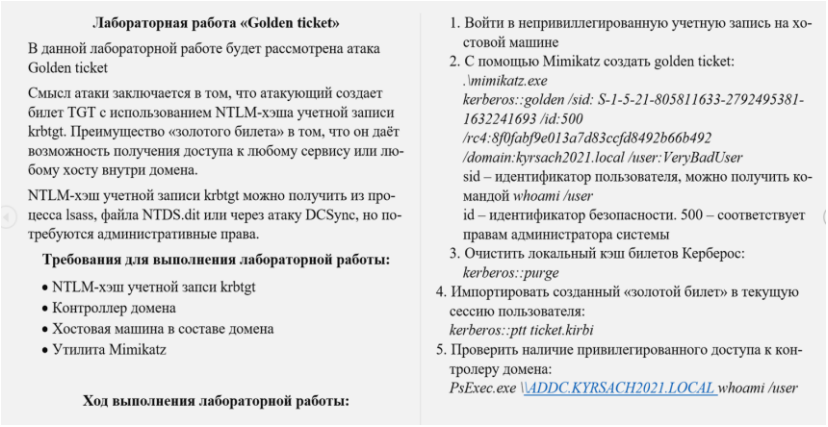
Было разработано 7 лабораторных работ на основе изученных атак и способов защиты от них, с использованием Windows систем:

- Взлом web-сервера с помощью sql-инъекции [4].
- Проведение html-инъекции.
- Атака Pass-the-hash [5].
- Kerberoasting в рамках протокола Kerberos [6].
- Dcsync — кража данных с помощью репликации домена.
- Overpass-the-hash и Pass-the-ticket, получение и использование билетов Kerberos.
- Golden Ticket — одна из наиболее сложных и красивых атак на Kerberos [7].

Каждая лабораторная работа состоит из краткой информации про атаку, указывается, почему возникает уязвимость в системе,

описываются необходимые требования для выполнения лабораторного задания, как правило на стенде уже все заранее установлено и подготовлено к выполнению задания. Далее предоставляется пошаговая инструкция для успешного выполнения атаки и в заключение указываются методы защиты от подобного рода атак.

На рис. 2 представлена часть лабораторной работы на атаку Golden Ticket. На рис. содержится краткая информация про атаку и необходимые требования для выполнения задания, ход выполнения, а также в лабораторной работе описана защита от атаки. Все лабораторные построены по такому принципу.



Лабораторная работа «Golden ticket»

В данной лабораторной работе будет рассмотрена атака Golden ticket

Смысл атаки заключается в том, что атакующий создает билет TGT с использованием NTLM-хэша учетной записи krbtgt. Преимущество «золотого билета» в том, что он даёт возможность получения доступа к любому сервису или любому хосту внутри домена.

NTLM-хэш учетной записи krbtgt можно получить из процесса lsass, файла NTDS.dit или через атаку DCSync, но потребуются административные права.

Требования для выполнения лабораторной работы:

- NTLM-хэш учетной запси krbtgt
- Контроллер домена
- Хостовая машина в составе домена
- Утилита Mimikatz

Ход выполнения лабораторной работы:

1. Войти в непривиллегированную учетную запись на хостовой машине
2. С помощью Mimikatz создать golden ticket:
   .\mimikatz.exe
   kerberos::golden /sid: S-1-5-21-805811633-2792495381-1632241693 /id:500
   /rc4:8f0fabf9e013a7d83ccfd8492b66b492
   /domain:kyrsach2021.local /user:VeryBadUser
   sid – идентификатор пользователя, можно получить командой *whoami /user*
   id – идентификатор безопасности. 500 – соответствует правам администратора системы
3. Очистить локальный кэш билетов Керберос:
   kerberos::purge
4. Импортировать созданный «золотой билет» в текущую сессию пользователя:
   kerberos::ptt ticket.kirbi
5. Проверить наличие привилегированного доступа к контролеру домена:
   PsExec.exe \\ADDC.KYRSACH2021.LOCAL whoami /user

Рис. 2. Пример лабораторной работы “Golden Ticket”

Выполнение данной атаки позволяет получить доступ к любому сервису или хосту внутри домена. Пример вывода, при успешном выполнении атаки представлен на рис. 3.

Рис. 3. Выполнение лабораторной работы “Golden Ticket”

Была проведена апробация лабораторного практикума в рамках дисциплины «Управление информационной безопасностью» в группе

студентов 5 курса (КБ177). После апробации лабораторных работ был проведен опрос, мы спрашивали, удобно ли пользоваться инфраструктурой (рис. 4), что понравилось при работе со стендом, не было ли ошибок в работе стенда, и чтобы студенты хотели изменить или добавить. В целом, по работе стенда и созданным лабораторным работам студенты отозвались положительно.

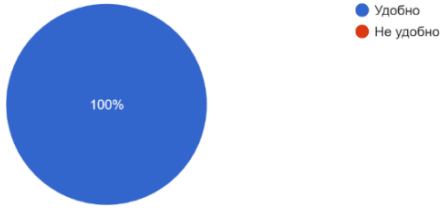


Рис. 4. Диаграмма с ответами на вопрос «удобно ли было использовать виртуальный стенд при работе с лабораторными работами»

Результаты. Результатом работы стал виртуальный стенд с реализованной ИТ-инфраструктурой, подобной инфраструктуре реальной организации, а также комплекс лабораторных работ по пентестингу и защите компонентов созданной инфраструктуры.

Заключение. В процессе выполнения работы удалось достичь всех поставленных задач. Была проделана большая работа по созданию полноценной, инфраструктуры, были рассмотрены актуальные уязвимости, атаки и методы защиты от них. На основе известных уязвимостей разработан комплекс лабораторных работ. Была произведена апробация и проанализирована обратная связь от студентов, а также рассмотрены векторы улучшения данного стенда.

СПИСОК ЛИТЕРАТУРЫ

1. Обзор площадок для практики навыков этичного хакера. — Текст : электронный // Хакер : [сайт]. — 2019. — URL: https://xakep.ru/2019/09/09/pentest-trainings/ (дата обращения: 31.03.2021).
2. Инфосистемы Джет. Атаки на домен / Инфосистемы Джет. — Текст : электронный // Habr : [сайт]. — 2019. — 21 июня. — URL: https://habr. com/ru/company/jetinfosystems/blog/449278 (дата обращения: 10.03.2022).

3. Методы защиты от mimikatz в домене Windows. — Текст : электронный // Winitpro : [сайт] — 2020. — 16 нояб. — URL: https://winitpro.ru/index.php/2017/08/24/metody-zashhity-ot-mimikatz-v-domene-windows/ (дата обращения: 25.04.2022).
4. Руководство по SQL-инъекциям: изучаем на примерах. — Текст : электронный // tgraph : [сайт] — 2018. — 22 окт. — URL: https://tgraph.io/Rukovodstvo-po-SQL-inekciyam-izuchaem-na-primerah-10-22?tg_rhash=6f689bcee5d75f (дата обращения: 10.04.2022).
5. Positive Technologies. Погружение в AD: разбираем продвинутые атаки на Microsoft Active Directory и способы их детекта / Positive Technologies. — Текст : электронный // Habr : [сайт]. — 2018. — 20 сент. — URL: https://habr.com/ru/company/pt/blog/423903/ (дата обращения: 20.04.2022).
6. Хантер Т. Разбираем атаки на Kerberos с помощью Rubeus / Т. Хантер. — Текст : электронный // Habr : [сайт]. — 2020. — 19 июня. — URL: https://habr.com/ru/company/tomhunter/blog/507140/ (дата обращения: 24.03.2022).
7. Принципы аутентификации по протоколу Kerberos — Текст : электронный // IT band : [сайт]. — 2017. — URL: http://itband.ru/2010/12/kerberos1/ (дата обращения: 14.03.2022).

Н. Н. Халтурин, Д. Д. Сухарев, А. В. Широких
Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА ЗАЩИЩЕННОГО МОБИЛЬНОГО ПРИЛОЖЕНИЯ «МОБИЛЬНЫЙ ОХОТИНСПЕКТОР»

Аннотация. *В рассматриваемой работе представлено мобильное приложение, разработанное для отечественных охотников, позволяющее безопасно, комфортно и законодательно заниматься охотой в России. Подробно описаны используемые при разработке технологии, принципы и рекомендации по информационной безопасности.*

Ключевые слова: *мобильная разработка, авторизация, API, Android, Flutter.*

Введение. В настоящее время многие люди стали пользоваться смартфонами повсеместно каждый день. Используя смартфоны,