УДК 004.738

Д. А. Шергин[1]✉, Д. Е. Пешков[1]

Разработка виртуального стенда для практического тестирования информационной безопасности Active Directory

[1]Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: shergindanil717@gmail.com

Аннотация. Статья посвящена разработке виртуального стенда для практического тестирования информационной безопасности Active Directory (AD), направленного на подготовку специалистов в области кибербезопасности. Актуальность исследования обусловлена широким распространением AD в корпоративных сетях и высокой частотой успешных атак из-за недостаточной защищенности ее компонентов. В работе использованы методы виртуализации (VMware Workstation 17 Pro) и моделирования корпоративной инфраструктуры, включающей виртуальные машины с различными операционными системами (Linux Ubuntu, Windows Server 2019, Windows 10). На стенде реализованы ключевые уязвимости AD, такие как слабая парольная политика, устаревшее ПО, некорректные настройки доступа и другие. Результатом исследования стал функциональный стенд, имитирующий реальную корпоративную сеть, который позволяет начинающим специалистам отрабатывать методы защиты и атаки в контролируемой среде. Стенд эффективно решает проблему нехватки практических навыков у начинающих специалистов.

Ключевые слова: информационная безопасность, безопасность инфраструктуры, Active Directory, виртуальный стенд

D. A. Shergin[1]✉, D. E. Peshkov[1]

Development of a virtual bench for practical testing of Active Directory information security

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: shergindanil717@gmail.com

Abstract. The article is devoted to the development of a virtual bench for practical testing of Active Directory (AD) information security aimed at training specialists in the field of cyber security. The relevance of the research is due to the widespread use of AD in corporate networks and the high frequency of successful attacks due to insufficient security of its components. The work uses virtualisation methods (VMware Workstation 17 Pro) and simulation of corporate infrastructure including virtual machines with different operating systems (Linux Ubuntu, Windows Server 2019, Windows 10). The stand implemented key AD vulnerabilities such as weak password policy, outdated software, incorrect access settings and others. The result of the research is a functional stand simulating a real corporate network, which allows novice specialists to practice defence and attack methods in a controlled environment. The stand effectively solves the problem of lack of practical skills among novice specialists.

Keywords: information security, infrastructure security, Active Directory, virtual bench

Введение

В мире стремительного роста и развития информационных систем и технологий все больше компаний старается наладить и выстроить все свои процессы, приведя их к единым стандартам и структуре. Компании активно внедряют Active Directory (далее – AD) для стандартизации процессов, так как эта технология удобна и популярна – ее используют 75 % крупнейших ИТ-компаний по всему миру. Однако управление привилегированным доступом в AD остается уязвимым местом: по данным Positive Technologies, в 64 % случаев злоумышленники могут получить доступ к конфиденциальной информации за 1–7 дней. Отсюда следует, что существует проблема в нехватке грамотных специалистов для оценки защищенности Active Directory и ее компонентов. Исходя из данной проблемы, было принято решение о разработке виртуального стенда для практического тестирования информационной безопасности Active Directory.

Актуальность

Active Directory – это служба каталогов, разработанная компанией Microsoft для Windows-доменных сетей. Она представляет собой централизованную и стандартизированную систему, которая автоматизирует управление пользовательскими данными, безопасностью и ресурсами сети.

Основные функции данной технологии:

- управление учетными записями пользователей;
- аутентификация и авторизация;
- групповые политики;
- управление ресурсами сети.

Active Directory является основой для управления большей части ресурсов организаций, использующих инфраструктуру Windows. Статистика, которую приводят Microsoft, показывает, что число организаций использующий данную технологию превысило 12,8 млн., а количество пользователей достигло более 950 млн., данные показатели выросли за последние 5 лет на 30 и 45 процентов соответственно, а из списка 500 крупнейших компаний по версии Fortune около 90 % из них используют AD [1].

Однако несмотря на достаточную защищенность данной технологии, многие компании не осуществляют надлежащей безопасной настройки данной технологии, что приводит к компрометации корпоративных ресурсов и активов компаний.

Так исходя из отчета PT по итогам аудита информационной безопасности за 2023 год в 100 % проектов, в которых проводилось внутреннее тестирование на проникновение, удалось получить контроль над доменом.

В 81 % проектов общий уровень защищенности был определен как низкий.

Самое быстрое получение максимальных привилегий в домене Active Directory – 6,5 часов после начала проведения работ по внутреннему пентесту, в остальных этот показатель варьируется от 1 до 7 дней. В 64 % проектов злоумышленник мог бы получить несанкционированный доступ к важной конфи-

денциальной информации. В некоторых случаях эта информация являлась интеллектуальной собственностью или служебной перепиской сотрудников.

Количество шагов требуемых для получения максимальных привилегий в домене составило до 8 шагов в 40 % случаях, что является достаточно критичным показателем и ведет к быстрой компрометации корпоративной сети компании [2].

Вышеперечисленные тезисы показывают, что несмотря на удобство и популярность использования Active Directory многими компаниями, не каждая компания уделяет должное внимание безопасности этой технологии, что может привести к компрометации корпоративных ресурсов и активов компаний. Отсюда следует, что существует проблема в нехватке грамотных специалистов для оценки защищенности Active Directory и ее компонентов. Исходя из данной проблемы, было принято решение о разработке виртуального стенда для практического тестирования информационной безопасности Active Directory, который позволит студентам по направлению Информационная безопасность отработать свои знаний и умения на практике и получить практический опыт оценки защищенности Active Directory, приближенный к реальным условиям [3].

Актуальные уязвимости Active Directory

Опираясь на результаты пентеста (аудита информационной безопасности) 2023 года от компании Positive Technologies, которые представляют собой собранную статистику за целый год и ее полный анализ, можно выделить ключевые уязвимости [2, 4]. Данные уязвимости встречаются во время тестирования на проникновение инфраструктуры организаций и Active Directory в частности:

- слабая парольная политика;
- устаревшее ПО и протоколы;
- небезопасная конфигурация;
- некорректная настройка политик доступа.

Данный перечень охватывает большее количество атак, которые можно реализовать в рамках данных уязвимостей, которые способны привести к несанкционированному доступу в корпоративную сеть. В частности, компрометация учетной записи администратора способна повлечь за собой полный контроль над критически важными системами, утечку конфиденциальных данных и даже саботирование бизнес-процессов.

Использование неподдерживаемых версий программного обеспечения и устаревших криптографических протоколов представляет серьезную угрозу информационной безопасности и делает систему открытой для известных атак. Злоумышленники могут воспользоваться публично доступными эксплойтами. Кроме того, слабые протоколы шифрования позволяют перехватывать и модифицировать передаваемые данные, что особенно опасно при обработке персональной информации или финансовых транзакций.

Некорректная настройка серверов, баз данных и сетевого оборудования значительно увеличивает поверхность атаки. Распространенные ошибки включают

использование стандартных учетных записей с привилегированным доступом, оставление открытых портов для удаленного управления (RDP, SSH без защиты) и отсутствие сегментации сети [5]. Подобные упущения позволяют злоумышленникам относительно легко проникать в систему, перемещаться внутри нее и внедрять вредоносное ПО. Например, недостаточная защита интерфейса управления базой данных может привести к утечке всей хранимой информации, а некорректные настройки межсетевого экрана – к несанкционированному доступу извне [6].

Отсутствие строгого контроля над правами пользователей и избыточные привилегии создают условия для внутренних угроз и горизонтального перемещения злоумышленников в случае компрометации. Если сотрудники имеют доступ к ресурсам, не требующимся для их работы, это нарушает принцип минимальных привилегий и увеличивает риск утечки или повреждения данных. В частности, недостаточная сегментация сети позволяет злоумышленнику, получившему доступ к одной системе, быстро распространять влияние на другие узлы.

Практическая часть исследования

На начальном этапе создания стенда была определена основная цепочка атаки, которая будет заложена в стенде (рис. 1).

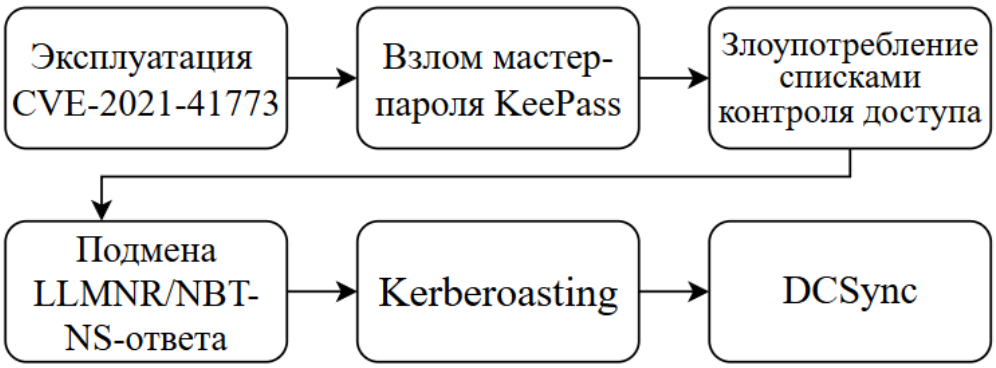

Рис. 1. Цепочка атаки

Для создания стенда было выбрано средство виртуализации VMware workstation 17 Pro. Данный инструмент позволяет запускать на одном физическом компьютере несколько виртуальных машин с различными операционными системами. В рамках стенда были настроены четыре виртуальные машины (далее – ВМ):

- ВМ №1 на базе операционной системы Linux Ubuntu 20.04;
- ВМ №2 на базе операционной системы Windows Server 2019;
- ВМ №3 на базе операционной системы Windows 10;
- ВМ №4 на базе операционной системы Windows 10.

В стенде было реализовано два ключевых этапа при которых атакующий должен сначала закрепиться внутри первой машины, а затем получить доступ в локальную сеть. Для этого на ВМ №1 было настроено два сетевых интерфейса, один из которых предоставляет выход в интернет, а второй позволяет взаимодействовать с машинами из локальной сети, которые в свою очередь не имеют выхода в интернет, находятся в одном домене и могут беспрепятственно взаимодействовать между собой. ВМ №2 выступает в роли контроллера домена (рис. 2).

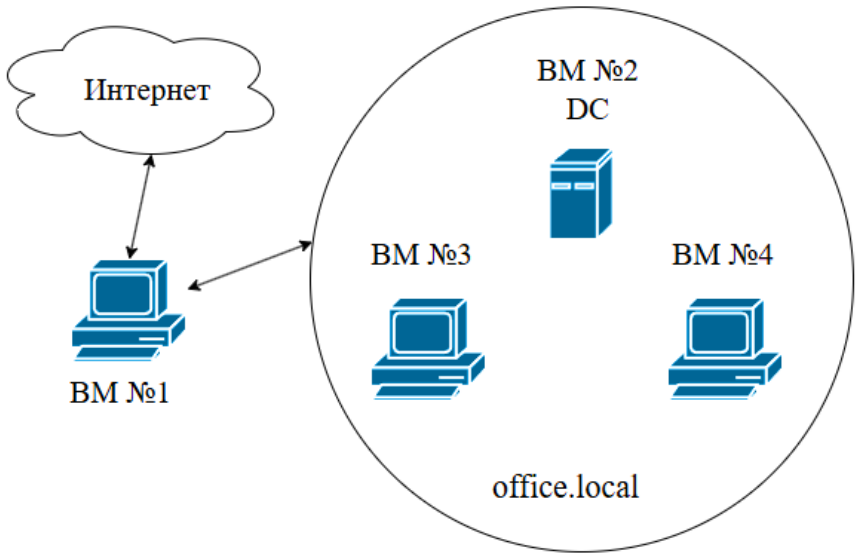

Рис. 2. Сетевое взаимодействие стенда

На ВМ1 было развернуто веб-приложение, использующее уязвимую версию веб-сервера Apache 2.4.49. А также был создан скрипт, который предоставляет информацию о сервере и использует протокол CGI. В дальнейшем это позволит проэксплуатировать уязвимость CVE-2021-41773 (рис. 3).

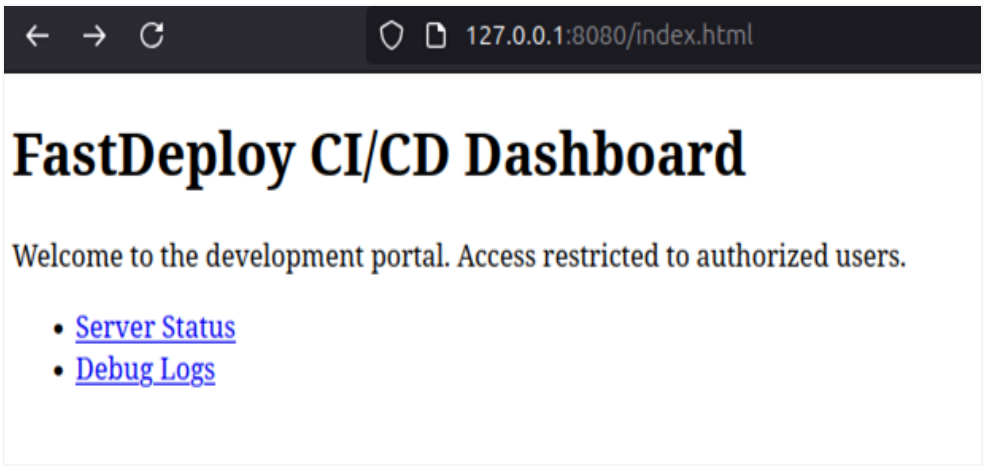

Рис. 3. Уязвимое веб-приложение

Также на ВМ1 был установлен менеджер паролей KeePass со слабым мастер-паролем, подверженным перебору в автономном режиме. Данный менеджер паролей хранит внутри себя учетные данные к удаленному рабочему столу пользователя на ВМ3 (рис. 4).

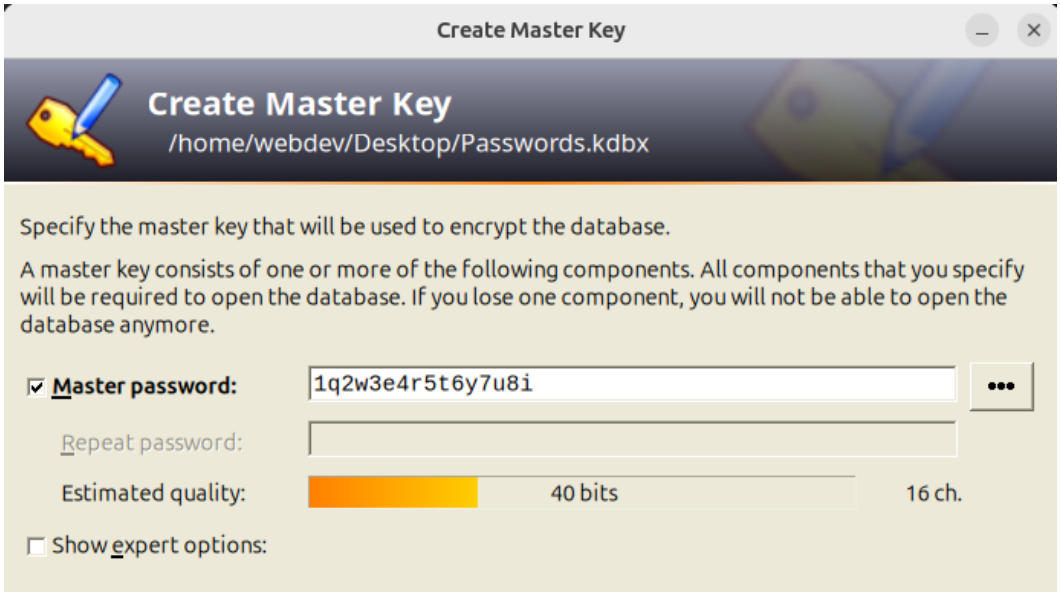

Рис. 4. Сетевое взаимодействие стенда

В домене office.local были созданы группы и соответствующие им пользователи. Данные группы имитируют разные отделы в компании, для каждой группы настроены свои политики доступа, некоторые из которых специально настроены некорректно что позволит повысить свои привилегии как вертикально, так и горизонтально табл. 1.

Таблица 1

Группы и пользователи в домене office.local

Название группы в домене	Имя пользователя
SupportTeam	Vlad_Support
	Victor_Support
Sellers	Petr_Seller
	Max_Seller
ExternalContractors	Iskra_manager
IT_Managers	Roman_IT_Manager
NetAdmins	Yra_SysAdmin
DataCenter	Alex_DataCenter
SeverOps	Vlad_Support
	Ivan_Support

В рамках домена была настроена общая сетевая папка, доступная всем пользователям по протоколу SMB. Внутри нее созданы дополнительные папки с различными уровнями доступа, которые в дальнейшем будут использоваться для задуманных атак [7].

Заключение

В результате был разработан виртуальный стенд, который представляет из себя некую корпоративную инфраструктуру вымышленной компании. Данный стенд можно использовать в качестве практической отработки навыков начинающих специалистов в области тестирования на проникновения Active Directory.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. IT-Lite. Обзор возможностей Active Directory: фундамент для инфраструктуры. – Текст : электронный // IT-Lite : [сайт]. – URL: https://www.it-lite.ru/blog/iaas/obzor-vozmozhnostey-active-directory/ – (дата обращения: 29.04.2025).

2. Итоги пентестов 2023. – Текст : электронный // Positive Technologies : [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2023/ – (дата обращения: 29.04.2025).

3. ADMINVPS. Что такое Active Directory в Windows. – Текст : электронный // ADMINVPS : [сайт]. – URL: https://adminvps.ru/blog/chto-takoe-active-directory-v-windows/ (дата обращения 12.05.2025).

4. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года. – Текст : электронный // Positive Technologies : [сайт]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ – (дата обращения: 22.04.2025).

5. J. Neumeier, A.L. Zelezinskii, O.V. Arhipova. Management of security of information in companies // Экономический вектор. 2023. №2. С.38-41.

6. Методика оценки угроз безопасности информации. – Текст : электронный // Федеральная служба по техническому и экспортному контролю : [сайт]. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения: 20.12.2023).

7. Скоропупов И. О., Бубнова А. А., Карманов И. Н. Методы проведения атак для получения прав администратора домена в Active Directory // Интерэкспо Гео-Сибирь. – Новосибирск: 2019. – Т. 6. – №. 1. – С. 187-192.