УДК 004.031.42

Аль-Джахдами Асад Саид Халфан,
Студент 2 курса
Институт «цифровых технологий, электроники и физики»
АлтГу «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Мансуров Александр Валерьевич, к.т.н., доцент кафедры ИБ
e-mail: mansurov.alex@gmail.com

МЕТОДЫ ПРОЕКТИРОВАНИЯ ЛАБОРАТОРИИ ПО ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ

Аннотация. В статье представлена информация о том, как создать безопасную виртуальную среду для лаборатории тестирования на проникновение с точки зрения положительных сторон создания виртуальной среды и потенциальных трудностей. В нем также будут рассмотрены практики создания виртуальной среды, технические характеристики устройств, которые вам понадобятся, их эффективность и с какими трудностями они, в связи с этим сталкиваются. В статье также будет рассказано о приложениях, используемых в работе виртуальной среды.

Annotation. The article provides information on how to build a secure virtual environment for a penetration testing lab in terms of the positives of creating a virtual environment and the potential difficulties. It will also review the practices of creating a virtual environment, the specifications of the devices you will need, their effectiveness, and what difficulties they face from that. The article will also talk about the applications used in the work of the virtual environment.

Ключевые слова: Лаборатории тестирования на проникновение, тестирование на проникновение, Pen-testing, информационная безопасность,

кибербезопасность, оценка безопасности, защита сети, лаборатория безопасной среды, инструменты тестирования на проникновение, инструмент Pen-testing, анализ приложений, анализ сети, анализ угроз.

Keywords: Penetration Testing Labs, Penetration Testing, Pen-testing, Information Security, Cyber Security, Security Assessment, Network protection, safe environment lab, Penetration testing tools, Pen-testing tool, application analysis, network analysis, threat analysis.

Введение

Традиционно, под пен-тестингом (или тестированием на проникновение) понимают проверку защищённости компьютерной системы, при которой моделируется реальная атака злоумышленника (хакера) [1]. Для тестирования на проникновение очень полезно создать собственную лабораторную среду, которая обеспечивает безопасную зону и виртуализирует реальную лабораторную среду.

Распространенные методы включают подготовку виртуальных операционных систем, таких как Window, Linux или любых других, с помощью таких программ, как Oracle VirtualBox VMWare workstation для windows, VMWare Fusion для Mac OS или Parallel desktop для Mac OS. Это программное обеспечение используется для виртуализации реальных машин, и мы будем использовать его для тестирования таких инструментов, как Metasploit для использования уязвимостей и Wireshark для анализа трафика и данных. Кроме того, можно загрузить готовые уязвимые ОС с таких платформ, как VulnHub,[2] чтобы потренироваться в использовании уязвимостей.

Introduction

Traditionally, pen-testing (or penetration testing) is understood as checking the security of a computer system, which simulates a real attack by an intruder (hacker) [1]. It is great to build your own lab environment for penetration testing where this environment provides a secure area and virtualizes the real lab environment.

The common methods include preparation of Virtual Operating Systems like Window, Linux, or any others by using software like Oracle VirtualBox VMWare workstation for windows, VMWare Fusion for Mac OS, or Parallel desktop on Mac OS. This software used to virtualize the real machines, and we will use it to evaluate a tool like Metasploit for exploiting the vulnerabilities and Wireshark for analyses the traffic and data. Also, you can load readymade vulnerable OS from platforms like VulnHub [2]to train yourself for exploit the vulnerabilities

Основные вопросы организации учебных лабораторий для пен-тестинга

Создание практической лаборатории тестирования на проникновение требует настройки узлов с несколькими операционными системами, приложениями и сетевыми настройками, которые воспроизводят реальную среду. Лаборатория должна быть изолирована от производственных сетей, масштабируема для будущих модернизаций и оснащена необходимыми инструментами. Ключевая задача заключается в обеспечении баланса между реалистичностью, безопасностью и функциональностью: инфраструктура должна отражать реальные системы для получения достоверных результатов тестирования при соблюдении этических и правовых норм. Сложность добавляют требования к ресурсам аппаратного и программного обеспечения, проблемы кроссплатформенной совместимости и необходимость постоянной интеграции возникающих угроз и средств защиты. Для поддержания

актуальности лабораторий их дизайн должен адаптироваться к конкретным целям тестирования, профилям угроз и системному опыту.[3]

Мы можем использовать различные типы лабораторий для создания безопасной среды и безопасногое тестирования приложений. Эти подходы зависят от цели лаборатории, типа угроз и знаний, связанных с целевыми системами.

На рисунке 1 показаны ключевые символические практики, направленные на процессы формирования лабораторий для проведения занятий по пен-тестингу:

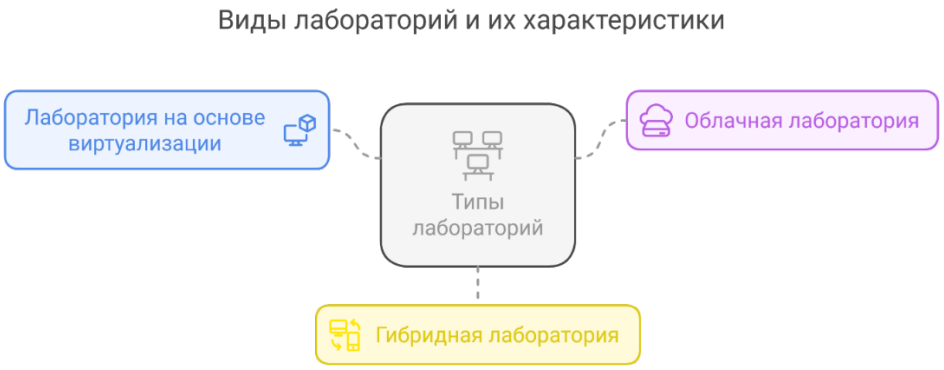

Рисунок 1. Ключевые практики создания лаборатории для пен-тестинга

В Таблице 1 кратко описаны основные достоинства и недостатки различных видов лабораторий для обучения тестированию на проникновение:

Таблица 1. Основные характеристики различных видов лабораторий для обучения тестированию на проникновение

Вид лаборатории	Описание	Преимущества	недостатки
Лаборатория на основе виртуализации	Связана с другой машиной, которая предоставит виртуальную машину на хосте для проведения тестирования на ней Примеры: VMWare, Parallel desktop	Недорогие деньги Гибкость Изолированный Масштабируемость	Ограниченные возможности Производительность, связанная с главной машиной Не полностью повторяет комплекс реальной среды
Лаборатория облачных	настройка и удаленное управление лабораторной средой Примеры: Yandex cloud, AWS Amazon, Azure Microsoft, Google Cloud	Доступность Масштабируемость Автоматическое обновление Производительность, не связанная с аппаратным обеспечением	Дорого Потенциальные проблемы с соблюдением нормативных требований и безопасностью Ограниченный контроль Требуется стабильный интернет [4]
Гибридная лаборатория	Combining physical and virtual components	Гибкость Тестирование устройств, таких как IoT и коммутаторы. Масштабируемость	Дорого Сложная настройка Требуются такие устройства, как коммутатор и маршрутизатор Управление как физическими, так и виртуальными устройствами [5]

Фокус на виртуальных лабораториях для тестирования на проникновение

Создание физической лаборатории для тестирования на проникновение требует значительных ресурсов, особенно для студентов. Виртуальные

лаборатории решают эту проблему, используя экономически эффективную виртуализацию, инструменты с открытым исходным кодом и готовые платформы для моделирования реалистичных сред. Такой подход позволяет минимизировать расходы на оборудование, сохраняя при этом надежные возможности тестирования.[6]

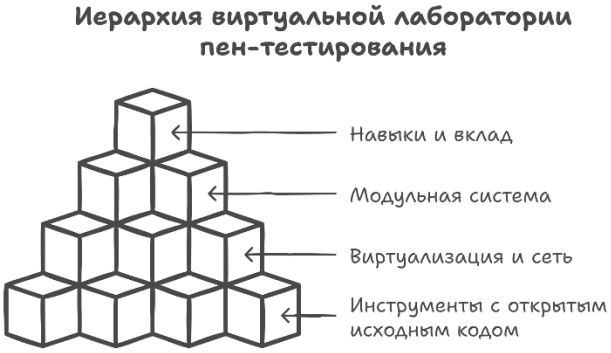

Рисунок 2 Иерархия виртуальной лаборатории пен-тестирования

Рисунок 2 демонстрирует иерархию, связанную с виртуальной лабораторией тестирования на проникновение. Она строится в виде пирамиды с четырьмя уровнями, каждый из которых представляет отдельный компонент:

1. Навыки и вклад (Skills and Contribution) – демонстрирует важность индивидуальных навыков и достижений в области кибербезопасности, поскольку они являются критически важными элементами в укреплении потенциала безопасности.
2. Модульная система (Modular System) —означает наличие гибкой системы, состоящей из взаимозаменяемых модулей, что позволяет легко совершенствовать и развивать структуру.
3. Виртуализация и сеть (Virtualization and Network) – здесь на первый план выходит виртуальная сеть в лаборатории, поскольку она играет решающую

роль в создании интегрированной операционной среды с различными сетями.

4. Инструменты с открытым исходным кодом (Open-Source Tools) – здесь на помощь приходят инструменты с открытым исходным кодом, обеспечивающие гибкость и универсальность архитектуры. К таким инструментам относятся Nmap, OpenVAS и другие, которые помогут нам создать лабораторию тестирования на проникновение.[7]

Лаборатория тестирования на проникновение должна учитывать все уровни подготовки, от начинающего до продвинутого. Определите такие цели, как тестирование безопасности веб-приложений, этичный взлом, анализ безопасности мобильных устройств и тестирование на проникновение в сеть. Требования к аппаратному обеспечению будут подробно описаны позже, но выбор платформы виртуализации (например, VirtualBox, VMware) имеет решающее значение. На этих платформах устанавливаются и эксплуатируются виртуальные машины (ВМ), включая операционные системы и намеренно уязвимые цели, например Metasploitable 2. Эти ВМ могут быть оснащены инструментами для тестирования на проникновение, такими как Nmap, Burp Suite, SQLmap и Hashcat, с учетом конкретных потребностей тестировщика.[7]

Лучшие методы создания лабораторий тестирования на проникновение включают в себя следующие позиции:

1. Изоляция среды от реальной сети.
2. Использование собственных конфигураций сети на виртуальных коммутаторах и маршрутизаторах.
3. Снимок виртуальной машины после завершения настройки и установки инструментов перед началом тестирования [8].

Процесс создания виртуализированной лаборатории и зон для каждого оборудования включает в себя следующие шаги:

1. Хост виртуализации. Основные позиции для среды виртуализации приведены в таблице 2.

Таблица 2. Сравнение среды виртуализации для лаборатории пен-тестирования

Платформа	**Доступна бесплатная версия**	**Описание**
VMware Workstation	Нет	Ведущая платформа виртуализации корпоративного уровня с расширенными возможностями.[9]
Microsoft Hyper-V	Да	Интеграция с Windows, обеспечивающая надежное решение для виртуализации серверов.[10]
Oracle VirtualBox	Да	Популярный гипервизор Type 2 с открытым исходным кодом, поддерживающий различные гостевые ОС.[11]
KVM (Kernel-based Virtual Machine)	Да	Модуль ядра Linux, позволяющий хосту запускать несколько виртуальных сред.[12]
Xen Project	Да	Для виртуализации серверов используется мощный гипервизор с открытым исходным кодом.[13]
EVE-NG	Да	Платная платформа управления эмуляторами с открытым исходным кодом на базе QEMU.[14]
Red Hat OpenShift Virtualization	Нет	Коммерческое решение, интегрирующее Kubernetes с виртуализацией.[15]

2. Зона атаки [16] – включает в себя решения, формирующие и обслуживающие рабочий инструментарий пен-тестера. Основной перечень составляющих зоны атаки приведен в таблице 3.

Таблица 3. Описание составляющих элементов зоны атаки.

Операционная система	**Доступна бесплатная версия**	**Описание**
Kali Linux	Да	Основанный на Debian дистрибутив с более чем 600 предустановленными инструментами для тестирования на проникновение и аудита безопасности.[17]
Metasploit	Да	система тестирования на проникновение с открытым исходным кодом, используемая для выявления и эксплуатации уязвимостей в системах.[18]
Nmap	Да	мощный инструмент сканирования сети, используемый для обнаружения хостов, служб и открытых портов в сети.
Burp Suite	Да	интегрированная платформа для тестирования безопасности веб-приложений.
сканер-вс	Нет	использовал сканер уязвимостей для выявления уязвимостей, неправильной конфигурации и проблем с соответствием требованиям в сетях и системах.[19]
OpenVAS	Да	Сканер уязвимостей с открытым исходным кодом, который обеспечивает функциональность, аналогичную сканер-вс. [20]
Wireshark	Да	Анализатор сетевых протоколов, перехватывающий и проверяющий пакеты, проходящие через сеть.[21]

3. Зона Целевая – включает в себя моделируемые и имитируемые компоненты корпоративной инфраструктуры, для которой проводится тестирование на

проникновение. Как правило, в этой зоне можно моделировать близкие к реальности или полностью соответствующие реальности сегменты корпоративной сети и корпоративную инфраструктуру, на которой располагаются защищаемые информационные системы и активы предприятия. Краткий перечень элементов приведен в таблице 4.

Таблица 4. Описание составляющих элементов целевой зоны.

Операционная система	**Доступна бесплатная версия**	**Описание**
Metasploitable	Да	ВМ на базе Linux с уязвимыми местами, используемая для обучения и тестирования инструментов.
Windows	Нет	Операционная система Microsoft для сервисов Clint. Вы можете найти ее в Интернете для тестирования. Для тестирования в среде Windows можно использовать виртуальную машину Windows (Windows 7 или Windows 11). [22]
Windows Server	Нет	Операционная система для управления клиентом в сети компании. Для тестирования служб сервера можно использовать Windows Server 2016 или более новые версии.[23]
Ubuntu	Да	Операционная система с открытым исходным кодом используется в качестве клиента и сервера.[24]
V-Switch /Router	Да	Виртуальный коммутатор или маршрутизатор как часть инструмента эмуляции может быть настроен.

Подготовка лаборатории тестирования на проникновение - важный шаг, гарантирующий, что среда способна выполнять лабораторную работу на ней. В этом разделе будут описаны требования к лабораторной среде в трех нормативных вариантах, и в зависимости от потребностей тестировщика на проникновение можно выбрать наиболее подходящее для него исполнение. В

таблице 5 приведены требования к аппаратной составляющей для развертываемой лаборатории [25].

Таблица 5. Аппаратные требования для развертываемой лаборатории пен-тестинга.

Категория	Минимальные	Рекомендуемые	наилучшей производительности
RAM	8 ГБ	16 ГБ	32 ГБ
жесткого диска Тип/размер	HDD / 500 ГБ	SSD / 1 ТБ	SSD NVMe / 2 ТБ
Процессор	i5 9th Генерации /Ryzen 5	i7 10th Генерации / Ryzen 7	i9 12th Генерации / Ryzen 9
Core	6 Core	8 core или больше	20 Core или больше
Скорость сети	1 Гбит/с Ethernet/Wi-Fi	1 Гбит/с Ethernet /Wi-Fi	10 Гбит/с Ethernet
NIC	1 карта	2 карты	2 карты или более
Монитор нуждаться	Не надо	1 если надо	2 или более

Заключение

В заключение следует отметить, что лаборатория тестирования на проникновение — это не просто техническая среда, а безопасное место, где специалисты по безопасности совершенствуют свои навыки, оттачивают стратегии и разрабатывают новые решения. Инвестируя в мощную лабораторную среду, студенты или организации могут повысить уровень своей кибербезопасности, защитить критически важные активы и быть на шаг впереди противников во все более сложном цифровом мире.

Литература

1. Ashraf, Q. M., & Habaebi, M. H. (2013). Towards Islamic ethics in professional penetration testing. *Revelation and Science*, *3*(2). (дата обращения 25.03.2025)
2. Vulnerable Pentesting Lab Environment: 1. Retrieved from https://www.vulnhub.com/entry/vulnerable-pentesting-lab-environment-1,737/ . (дата обращения 10.03.2025)
3. Engebretson, P. (2013). The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy. Elsevier. (дата обращения 11.03.2025)
4. Retrieved from https://aws.amazon.com/security/penetration-testing/ . (дата обращения 12.03.2025)
5. Konak, A., Clark, T., & Nasereddin, M. (2013, March). Best practices to design hands-on activities for virtual computer laboratories. In *2013 IEEE Integrated STEM Education Conference (ISEC)* (pp. 1–7). IEEE. (дата обращения 16.03.2025)
6. Kim, P. (2014). The hacker playbook 3: Practical guide to penetration testing (pp. 328–362). Secure Planet LLC. (дата обращения 20.03.2025)
7. de Leon, D. C., Jillepalli, A. A., House, V. J., Alves-Foss, J., & Sheldon, F. T. (2018). Tutorials and laboratory for hands-on OS cybersecurity instruction. *Journal of Computing Sciences in Colleges, 34*(1), 242–254. (дата обращения 18.03.2025)
8. Konak, A., Clark, T., & Nasereddin, M. (2013, March). Best practices to design hands-on activities for virtual computer laboratories. In *2013 IEEE Integrated STEM Education Conference (ISEC)* (pp. 1–7). IEEE. (дата обращения 19.03.2025)

9. Fusion and Workstation. Retrieved from https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion . (дата обращения 28.03.2025)
10. Hyper-V Server 2019. Retrieved from https://www.microsoft.com/en-us/evalcenter/evaluate-hyper-v-server-2019 . (дата обращения 28.03.2025)
11. Downloads. Retrieved from https://www.virtualbox.org/wiki/Downloads . (дата обращения 28.03.2025)
12. Downloads. Retrieved from https://www.linux-kvm.org/page/Downloads . (дата обращения 28.03.2025)
13. Retrieved from https://xenproject.org/resources/downloads/ . (дата обращения 28.03.2025)
14. Download. Retrieved from https://www.eve-ng.net/index.php/download/
15. Try Red Hat OpenShift. Retrieved from https://www.redhat.com/en/technologies/cloud-computing/openshift/try-it . (дата обращения 28.03.2025)
16. Lee, I. (2025). 15 must-have tools for penetration testing in 2025. Retrieved from https://www.wallarm.com/what/15-must-have-tools-for-penetration-testing# . (дата обращения 07.04.2025)
17. Get Kali. (2024). Retrieved from https://www.kali.org/get-kali/#kali-platforms. (дата обращения 11.04.2025)
18. Metasploitable. (2024). Retrieved from https://sourceforge.net/projects/metasploitable/. (дата обращения 11.04.2025)
19. Главная страница: Система комплексного анализа защищенности “Сканер-ВС.” Retrieved from https://scaner-vs.ru/. (дата обращения 11.04.2025)

20. Greenbone Community Portal. (2025). Retrieved from https://community.greenbone.net/?spm=a2ty_o01.29997173.0.0.5223c9219nXuiw. (дата обращения 11.04.2025)
21. Wireshark · Go Deep. Retrieved from https://www.wireshark.org/?spm=a2ty_o01.29997173.0.0.5223c9219nXuiw. (дата обращения 11.04.2025)
22. Retrieved from https://answers.microsoft.com/en-us/windows/forum/all/download-win-7-trial/264301c7-68a2-45d6-8bf8-7ee64c5ded52. (дата обращения 12.04.2025)
23. Windows Server 2019. Retrieved from https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019. (дата обращения 12.04.2025)
24. Get Ubuntu: Download. Retrieved from https://ubuntu.com/download. (дата обращения 12.04.2025)
25. PassMark Software. Retrieved from https://www.passmark.com/?srsltid=AfmBOoo7MWsI7AeOihH6lc6zhGRdG5lwN0FSVjJXT5768bYa_Rz0EhEs. (дата обращения 17.04.2025)