ПОДГОТОВКА ЧТО ВАМ НУЖНО

ПРЕЖДЕ ЧЕМ НАЧАТЬ

// Минимальные характеристики для полноценной работы в хакерской лаборатории

Вам не нужен суперкомпьютер. Ноутбука среднего уровня, выпущенного с 2018 года, более чем достаточно. Вся лаборатория работает внутри виртуальных машин — изолированных от вашей основной операционной системы.



Минимум 8 ГБ ОЗУ

16 ГБ — идеально: позволит запускать 2 виртуальные машины одновременно для атакующих/защитных лабораторий



50 ГБ свободного места на диске

ISO-образ Kali весит 4 ГБ, установленная система занимает ~25 ГБ



Виртуализация включена в BIOS

Включите Intel VT-x или AMD-V — обычно по умолчанию на современных машинах



Основная ОС: Windows, macOS или Linux

VirtualBox работает на всех трёх платформах — ваша основная система остаётся нетронутой

01 ШАГ ПЕРВЫЙ

УСТАНОВИТЕ VIRTUAL BOX

// Движок, который запускает ваши виртуальные машины — 100% бесплатно

VirtualBox — это гипервизор с открытым исходным кодом. Он позволяет запускать целую операционную систему внутри окна на вашем экране. Всё, что происходит в виртуальной машине, остаётся внутри неё — ваша основная система в безопасности.



VirtualBox 7.x

virtualbox.org/wiki/Downloads

Windows / macOS / Linux — ~110MB

БЕСПЛАТНО

```
# Проверьте, включена ли виртуализация
$ egrep -c '(vmx|svm)' /proc/cpuinfo
4 — любое число больше 0 означает, что всё хорошо

# После установки — проверьте версию
$ VBoxManage --version
7.0.12r159484
```

~5 минут | Бесплатно навсегда | Все платформы

02 ШАГ ВТОРОЙ

СКАЧАЙТЕ_ KALI LINUX

// Операционная система хакера — более 600 предустановленных инструментов

Kali Linux создана командой Offensive Security специально для тестирования на проникновение. В ней есть всё необходимое — Nmap, Burp Suite, Metasploit, Wireshark — предустановлены и готовы к работе.



Kali Linux 2024.x (Installer)

kali.org/get-kali – Installer AMD64

4.0 GB – проверьте SHA256 после загрузки!

БЕСПЛАТНО

```
# Совет профи: используйте предустановленный образ VirtualBox
# Без ручной установки – просто импортируйте и загрузитесь
kali.org/get-kali/#kali-virtual-machines

# Всегда проверяйте загруженный файл!
$ sha256sum kali-linux-2024.3.iso
a8f2c94e... ⟵ сравните с официальным сайтом
```

~10 МИН СКАЧИВАНИЕ

600+ ИНСТРУМЕНТОВ

НА ОСНОВЕ DEBIAN

03 ШАГ ТРЕТИЙ

СОЗДАЙТЕ КОНФИГУРАЦИЮ ВИРТУАЛЬНОЙ МАШИНЫ

// Правильные настройки с самого начала — это важно

Правильные настройки виртуальной машины обеспечивают стабильную работу Kali и изоляцию от вашей сети. Используйте эти точные значения — скопируйте их напрямую.

Новые настройки виртуальной машины:

Имя	:	KaliLab-2024
Тип	:	Linux – Debian (64-bit)
Оперативная память	:	4096 МБ (мин) 8192 МБ (рекомендовано)
Процессоры	:	2 (или половина от ваших ядер)
Диск	:	50 ГБ – с динамическим выделением
Сеть 1	:	NAT – доступ к интернету
Сеть 2	:	Только узел – изоляция лаборатории

NAT = интернет

Только узел = сеть лаборатории

~5 мин

04 ШАГ ЧЕТВЁРТЫЙ

ЗАГРУЗКА И УСТАНОВКА KALI

// Следуйте этим настройкам точно во время установки

Подключите ISO-образ к виртуальной машине, загрузитесь с него и следуйте установщику. Это единственные настройки, в которых вам нужно принять решение — всё остальное можно оставить по умолчанию.

- **Выберите:** Графическая установка — проще всего для новичков
- **Язык:** English — обеспечивает единообразие команд в терминале
- **Имя хоста:** kali — простое имя, отображается в терминале
- **Имя пользователя:** что угодно — не используйте своё настоящее имя
- **Разметка диска:** Guided — использовать весь диск — без сложности с двойной загрузкой
- **Окружение рабочего стола:** XFCE — самое лёгкое по потреблению памяти, рекомендуется профессионалами

~10–15 МИН УСТАНОВКА

XFCE = САМОЕ БЫСТРОЕ

05 ШАГ ПЯТЫЙ

ПЕРВАЯ НАСТРОЙКА ПОСЛЕ ЗАГРУЗКИ

// Выполните эти команды сразу после установки

Первое, что нужно сделать после загрузки — обновите систему. Затем добавьте целевую машину. Это базовая настройка, которую каждый пентестер выполняет перед началом работы.

```
# 1. Обновите все пакеты — делайте это всегда в первую очередь
┌(kali@kali)-[~]
└$ sudo apt update && sudo apt upgrade -y

# 2. Установите дополнения гостевой ОС VirtualBox (полный экран)
└$ sudo apt install -y virtualbox-guest-x11

# 3. Проверьте, что ключевые инструменты готовы к работе
└$ nmap --version
Nmap 7.94 — готово!
└$ msfconsole --version
Framework 6.4.0-dev — готово!
```

~5 МИНУТ

ЛАБОРАТОРИЯ ГОТОВА К РАБОТЕ

БОНУС ДОБАВЬТЕ ЦЕЛЕВУЮ МАШИНУ

METASPLOITABLE 2

// Целевая уязвимая VM для безопасной — и законной — атаки

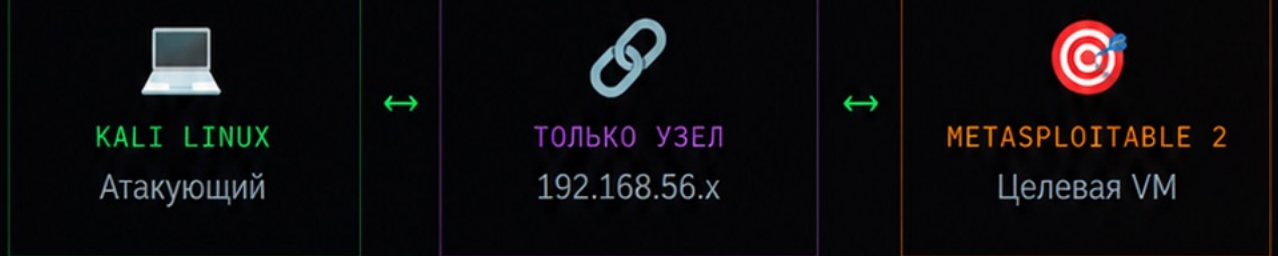
Metasploitable 2 — это виртуальная машина, созданная специально для взлома. На ней запущены десятки намеренно уязвимых сервисов. Разместите её в своей изолированной сети — и ваша лаборатория готова.

Metasploitable 2

sourceforge.net/projects/metasploitable

~900MB — импортируйте как существующую VM в VirtualBox

БЕСПЛАТНО



ЗАКОННО ДЛЯ АТАК

ИЗОЛИРОВАННАЯ СЕТЬ

30+ УЯЗВИМОСТЕЙ

// вступай в

ЛЕГИОН

СТАНЬ ЧАСТЬЮ ЛЕГИОНА

ВСТУПАЙ В ЛЕГИОН

учись. исследуй. взламывай. расти вместе с нами.

ЛЕГИОН — это сообщество энтузиастов кибербезопасности, объединённых одной целью — становиться лучше каждый день и менять цифровой мир к лучшему.

ОБУЧЕНИЕ
эксклюзивные гайды, статьи и разборы

ПРАКТИКА
лабы, машины, CTF и реальные кейсы

СООБЩЕСТВО
единомышленники, поддержка и нетворк

РОСТ
твои навыки — твоя сила

// ПОДПИСЫВАЙСЯ И РАЗВИВАЙСЯ С НАМИ

Подписывайтесь на @lionsoulbatyshchikov, чтобы получать больше инсайтов и обновлений из мира AI/кибербезопасности.

ПОДПИСАТЬСЯ НА @LIONSOULBATYSHCHIKOV

СОХРАНИТЬ ПОСТ