# План обучения пентесту с нуля и до профессионала

## Основы. Начальный уровень: сети

Книга: Николай Кузьменко: Компьютерные сети и сетевые технологии . Подробнее: Книга охватывает очень широкий круг вопросов. Отлично подойдет в качестве первой книги по сетям, а так же познакомит с разными вещами,такими как: рейдмасивы, как работает сервер и т.д.

Книга: Э.Таненбаум, Д.Уэзеролл "Компьютерные сети" 5-е изд. (2012)
Подробнее: В книге последовательно изложены основные концепции по компьютерным сетям, определяющие современное состояние и тенденции. Лучшее что можно найти на русском языке. Стоит прочесть после Кузьменко, в качестве закрепления материала.

YouTube канал: Andrey Sozykin
Подробнее: Прошерстив русский YouTube, понял, что данный канал - это лучшее что можно посмотреть по этой теме.

Книга: Официальное руководство Cisco по подготовке к сертификационным экзаменам
Подробнее: Первый шаг к выполнению практических заданий. Читать параллельно с ниже приведёнными курсами.

YouTube плейлист: Настройка cisco от простого к сложному

YouTube плейлист: Курс молодого бойца CCNA cisco
Подробнее: Начинаем практику по работе с коммутаторами и маршрутизаторами Cisco. Работа с другими коммутаторами, как правило,
ничем принципиально не отличается, кроме синтаксиса команд и более скудным функционалом.

Книга: Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях
Подробнее: Умение работать с Wireshark и tcpdump является обязательный навыком, как сетевого инженера, так и начинающего пентестера.

Инструменты для практики: cisco packet tracer, eve-ng, wireshark, tcpdump

## Операционные системы

Книга: Linux от новичка к профессионалу 6 издание
Подробнее: Очень хорошая, но объемная книга, которая охватывает большое количество дистрибутивов и практик по работе с ними.

Книга: Командная строка Linux. Полное руководство. 2-е межд. изд
Подробнее: Отличная книга, в которой описано множество трюков по работе с Linux

Книга: Руссинович Марк, Соломон Дэвид "Внутреннее устройство Windows"

Подробнее: Книга охватывает очень много моментов, которые будут полезны будущему пентестеру. Есть отдельные главы посвященные безопасности ОС.

## Инструменты для практики: Повседневное использование ОС и решение возникающих проблем

### Программирование

Книга: “Укус Питона” – “A Byte of Python”
Подробнее: Отличная книга для начинающих. Находится в свободном доступе.

Книга: Марк Лутц "Программирование на Python" 1-й ТОМ 4-ое издание
Подробнее: Та книга, с которой я начинал.

Книга: Марк Лутц "Программирование на Python" 2-й ТОМ 4-ое издание

Книга: Марк Лутц "Изучаем Python" 1-й ТОМ, 5-ое издание

Книга: Марк Лутц "Изучаем Python" 2-й ТОМ, 5-ое издание

YouTube канал: Олег Молчанов
Подробнее: Лучший русскоязычный канал, посвященный обучению программирования на Python

Инструменты для практики: Любая IDLE, которая угодна душе, их существует огромное множество. Очень важно постоянно писать код и пытаться с помощью программирования решать повседневные задачи.

## Мидл уровень

### Сети

Книга: TCP/IP. Сетевое администрирование
Подробнее: Обязательная к прочтению книга. Две главы посвящены безопасности и разрешению проблем.

Книга: Системное и сетевое администрирование. Практическое руководство
Подробнее: Даёт огромные знания по BIND и DNS

Обязательно изучить как работают протоколы:

- TCP/IP, Ethernet, MPLS, IP SLA, QoS и т.п
- Знания в области IP маршрутизации, знать как работаю протоколы OSPF, EIGRP, BGP
- Знания в L2 и и понимание работы протоколов STP, RSTP, VTP, link-aggregation
- Понимание принципов работы MPLS

### Операционные системы

Книга: Линн С. «Администрирование Microsoft Windows Server 2012»

Подробнее: Дает представление о работе серверов на базе Windows

Книга: Unix и Linux. Руководство системного администратора
Подробнее: Возможно, не лучшее что есть, но в принципе можно взять и что-то другое по администрированию линуксовых систем.

Книга: «FreeBSD. Подробное руководство»
Подробнее: Это, можно сказать, библия для *nix администратора

YouTube канал: Kirill Semaev
Подробнее: Лучшее, что есть на русском YouTube. Очень хорошо объясняет, есть практические задания.

Практика: Постройка своей "корпоративной сети" среднего офиса на виртуальных машинах.

## Программирование

Книга: Грокаем алгоритмы. Иллюстрированное пособие для программистов и любопытствующих
Подробнее: Алгоритмы знать просто обязательно.

Книга: Чистый код. Создание, анализ и рефакторинг
Подробнее: -

Сайт:


Рефакторинг и Паттерны проектирования
Рефакторинг — это контролируемый процесс улучшения вашего кода, без написания новой функциональности. Паттерны проектирования описывают типичные способы решения часто встречающихся проблем при проектировании программ.
refactoring.guru

Подробнее: Сайт посвящён тёмным материям программирования: рефакторингу, паттернам проектирования,
принципам SOLID и другим важным темам из мира программирования.

Книга: Погружение в ПАТТЕРНЫ ПРОЕКТИРОВАНИЯ
Подробнее: Паттерны важно знать, потому что они помогают решать многие задачи, а так же
для понимания, что происходит в коде других разработчиков.

Практика: Реализовать свой собственный проект, который будет нести импакт. (пример: ботнет, крупный интернет магазин, цмс и т.д.)

## Пентест

По пентесту очень сложно дать какие-то конкретные темы, ибо поиск уязвимостей больше похож на работу детектива или художника.
Все на данный момент описанные методы являются лишь более рекомендательными, чем обязательными. При пентесте очень важен опыт, который можно получить только практикой. Но вот что рекомендуется к ознакомлению:

- Занимайся хакингом с ловкостью порнозвезды
- Занимайся хакингом с ловкостью Бога
- Занимайся расследованием киберпреступлений как рок-звезда
- Занимайся хакингом как легенда
- Линукс глазами хакера и остальная серия книг "Глазами хакера"
- Certified Ethical Hacker Review Guide
- Metasploit: The Penetration Tester's Guide
- RTFM: Red Team Field Manual
- Искусство эксплойта 2ое издание
- Black Hat Python
- Вскрытие покажет! Практический анализ вредоносного ПО
- Kali Linux от разработчиков
- Основы веб-хакинга: Как зарабатывать деньги этичным хакингом
- OWASP документации
- DevOpsSec

Это только то, что я смог вспомнить.
Ресурсы для практики и оттачивания навыков:

- root-me
- xss-game
- Hack The Box
- bWAPP
- DVIA
- try2hack
- hackademic
- hack.me

Удачи в обучении! Возможно, гайд будет пополняться.