Основы кибербезопасности и этичный хакинг (Старт здесь!)

Эти книги — фундамент для понимания атак и защиты.

1. **The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition (Dafydd Stuttard, Marcus Pinto)**
    - **Описание: Библия тестирования веб-приложений.** Несмотря на год выпуска (2011), книга раскрывает фундаментальные концепции (SQLi, XSS, CSRF, логические уязвимости), которые остаются актуальными в 90% случаев. Лучший старт для веб-пентеста.
    - **Актуальность:** Принципы — вечные, технологии (типы атак) — актуальны, но требует дополнения изучением современных фреймворков (REST API, GraphQL, JWT).
2. **Penetration Testing: A Hands-On Introduction to Hacking (Georgia Weidman)**
    - **Описание:** Идеальная книга для **полного новичка**, который хочет стать этичным хакером. Автор проводит читателя по всем этапам: разведка, эксплуатация, пост-эксплуатация, написание отчетов. Много практических лабораторных работ.
    - **Актуальность:** Хорошая основа, но некоторые инструменты могут устареть. Важно понимать методологию, которую книга дает блестяще.
3. **Real-World Bug Hunting: A Field Guide to Web Hacking (Peter Yaworski)**
    - **Описание:** Современная жемчужина для тех, кто хочет **находить и эксплуатировать уязвимости в реальных веб-приложениях** (как это делают баг-хантеры). Книга построена на кейсах из программ Bug Bounty с объяснением логики атакующего.
    - **Актуальность: Высокая.** Охватывает современные типы уязвимостей (XXE, десериализация, проблемы бизнес-логики).

Продвинутые темы и эксплуатация уязвимостей

Для тех, кто освоил базу и хочет углубиться.

4. **The Hacker Playbook 3: Practical Guide To Penetration Testing (Peter Kim)**
    - **Описание:** Это не учебник, а именно **плейбук** — пошаговое руководство по проведению пентеста «от и до» в современных сетях (облака, обход EDR, фишинг). Много практических команд, примеров и сценариев.
    - **Актуальность: Очень высокая.** Серия постоянно обновляется. Это взгляд на современные инструменты и тактики (Red Team).
5. **Advanced Penetration Testing: Hacking the World's Most Secure Networks (Wil Allsopp)**
    - **Описание:** Книга для **профессионалов Red Team**. Фокус на таргетированных, скрытных атаках, социальной инженерии, создании кастомизированного вредоносного ПО и обходе самых сложных систем защиты. Не для начинающих.
    - **Актуальность:** Высокая для complex-атак, требующих нестандартного мышления.
6. **Black Hat Python, 2nd Edition & Gray Hat C# (Justin Seitz)**
    - **Описание:** Две must-have книги для **написания хакерского инструментария**. Python — для создания эксплойтов, сканеров, снифферов. C# — для работы в среде Windows, создания payload для .NET, анализа кода. Практическое программирование для пентестера.
    - **Актуальность: Высокая.** Языки и подходы остаются ключевыми в индустрии.

Низкоуровневый хакинг: реверс-инжиниринг и уязвимости ПО

Сердцевина поиска 0-day уязвимостей.

7. **Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation (Bruce Dang, Alexandre Gazet, Elias Bachaalany)**
    - **Описание:** Одна из лучших **практических книг по реверс-инжинирингу**. Разбирает дизассемблированный код, методы анализа, анти-отладку, работу с ядром Windows. Требует базового знания ассемблера и архитектуры процессоров.
    - **Актуальность:** Фундаментальные знания, не устаревающие со временем.
    - **The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd Edition (Chris Anley et al.)**

- **Описание: Классика эксплуатации.** Детально разбирает переполнение буфера, heap-спреи, форматные строки, эксплуатацию на разных ОС. Книга сложная, но дает глубочайшее понимание того, **как работают эксплойты на уровне памяти**.
- **Актуальность:** Принципы эксплуатации памяти (особенно в C/C++) актуальны, хотя современные защиты (ASLR, DEP, CFG) требуют изучения дополнительно.
- **Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly (Dennis Andriesse)**
    - **Описание:** Современный взгляд на анализ бинарных файлов. Учит не просто использовать IDA Pro, а **писать свои инструменты** на Python для автоматизации анализа, обфускации, поиска уязвимостей. Очень ценный практический навык.
    - **Актуальность: Очень высокая.**

Советы по изучению:

1. **Не читайте пассивно.** Устанавливайте виртуальные машины (VirtualBox/VMware), создавайте лаборатории (например, с помощью VulnHub, HackTheBox, TryHackMe), повторяйте все примеры из книг.
2. **Сочетайте книги с практикой.** Книга дает знания, а навык появляется только на практике. Решайте задачи на платформах CTF.
3. **Следите за актуальностью.** Подпишитесь на блог безопасности