ПРАКТИЧЕСКИЙ ГАЙД

ПОДХОДИТ НОВИЧКАМ

Взлом — не магия. Это процесс.

Реальный penetration test проходит в 7 фаз. Разбираем каждую из них с нуля — просто и по делу.



01 РАЗВЕДКА
Сбор информации и определение целей.

02 РЕКОН
Глубокая проверка и уточнение найденных данных.

03 СКАНИРОВАНИЕ
Поиск открытых портов, сервисов и уязвимостей.

04 АНАЛИЗ
Оценка найденных уязвимостей и возможных путей атаки.

05 ЭКСПЛУАТАЦИЯ
Использование уязвимостей для получения доступа.

06 ПОСТ-ЭКСПЛУАТАЦИЯ
Закрепление, повышение привилегий и движение по сети.

07 ОТЧЁТ
Документирование результатов и рекомендации по устранению рисков.

7 ФАЗ · 15 СЛАЙДОВ · КАЖДОЕ ПОНЯТИЕ ОБЪЯСНЯЕМ

ЛИСТАЙ ДАЛЬШЕ »

@lionsoulbatyshchikov

СНАЧАЛА ОПРЕДЕЛЕНИЕ

Что такое pentest?

Pentest — это санкционированная, имитированная атака на систему, чтобы найти её слабые места до того, как это сделает реальный злоумышленник.



ЗЛОУМЫШЛЕННИК

ДОСТУП
Никакого разрешения

ЦЕЛЬ
Украсть, навредить, получить выгоду

СЛЕДЫ
Скрывает свои действия

ЧЕМ ЗАКАНЧИВАЕТСЯ
Реальным инцидентом

PENETRATION TESTER

ДОСТУП
Официальное разрешение и чёткие правила (scope)

ЦЕЛЬ
Найти уязвимости, чтобы их исправить

СЛЕДЫ
Документирует всё

ЧЕМ ЗАКАНЧИВАЕТСЯ
Отчётом с рекомендациями



ОДНИ НАВЫКИ · РАЗНЫЕ ПРАВИЛА

ПОЧЕМУ КОМПАНИИ ПЛАТЯТ ЗА PENTEST

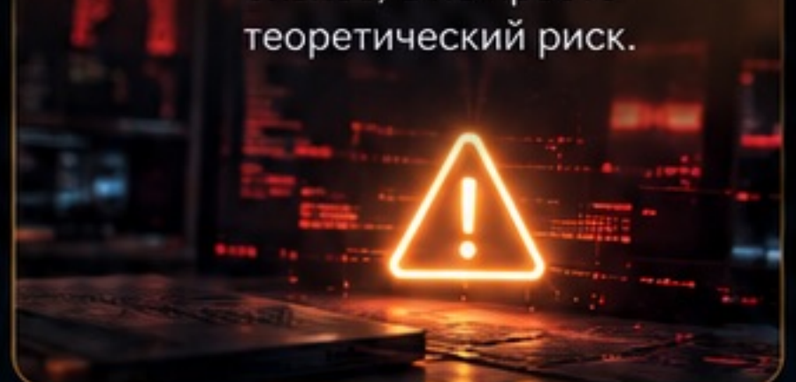
НАЙТИ ПРОБЛЕМЫ ЗАРАНЕЕ

Обнаружить слабые места до того, как их найдёт злоумышленник.



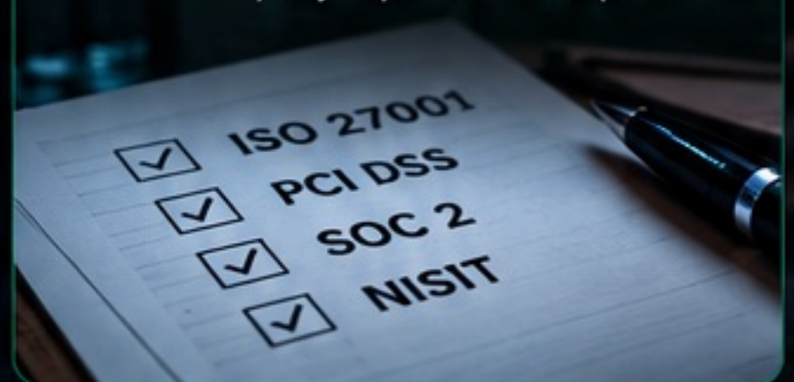
ПОКАЗАТЬ РЕАЛЬНЫЙ РИСК

Доказать влияние уязвимостей на реальный бизнес, а не просто теоретический риск.



СООТВЕТСТВОВАТЬ ТРЕБОВАНИЯМ

Многие стандарты безопасности требуют регулярного тестирования.



ГЛАВНОЕ ПРАВИЛО Тест без разрешения — это не исследование, а преступление. Pentest проводится только с согласия владельца системы.

БОЛЬШАЯ КАРТИНА

7 фаз. Один процесс.

Любой pentest идёт по этому же пути. Названия шагов могут отличаться, но порядок всегда один.

1

Подготовка (Pre-Engagement)

Определяем цели, границы (scope), сроки, правила и получаем письменное разрешение.

→ SIGNED SCOPE



2

Разведка (Reconnaissance)

Собираем публичную информацию о цели (OSINT) — тихо и аккуратно.

→ TARGET PROFILE



3

Сканирование и перечисление (Scanning & Enumeration)

Находим активные системы, открытые порты и запущенные сервисы.

→ OPEN PORTS

```
> nmap -sC -sV target.com
PORT     STATE  SERVICE   VERSION
22/tcp   open   ssh       OpenSSH 9.2p1
80/tcp   open   http      nginx 1.24.0
443/tcp  open   https     nginx 1.24.0
```

4

Анализ уязвимостей (Vulnerability Analysis)

Сопоставляем найденное с известными уязвимостями и ранжируем по риску.

→ RANKED FLAWS



5

Эксплуатация (Exploitation)

Используем уязвимость для получения доступа. Доказываем, но не наносим вред.

→ PROOF OF ACCESS

```
$ exploit ... ....
[+] Exploit successful
[+] Got shell (user: www-data)
$ _
```

6

Пост-эксплуатация (Post-Exploitation)

Проверяем, насколько далеко можно зайти: привилегии, lateral movement, влияние на бизнес.

→ IMPACT MAP



7

Отчёт (Reporting)

Фиксируем все находки, даём рекомендации, чтобы их реально исправили.

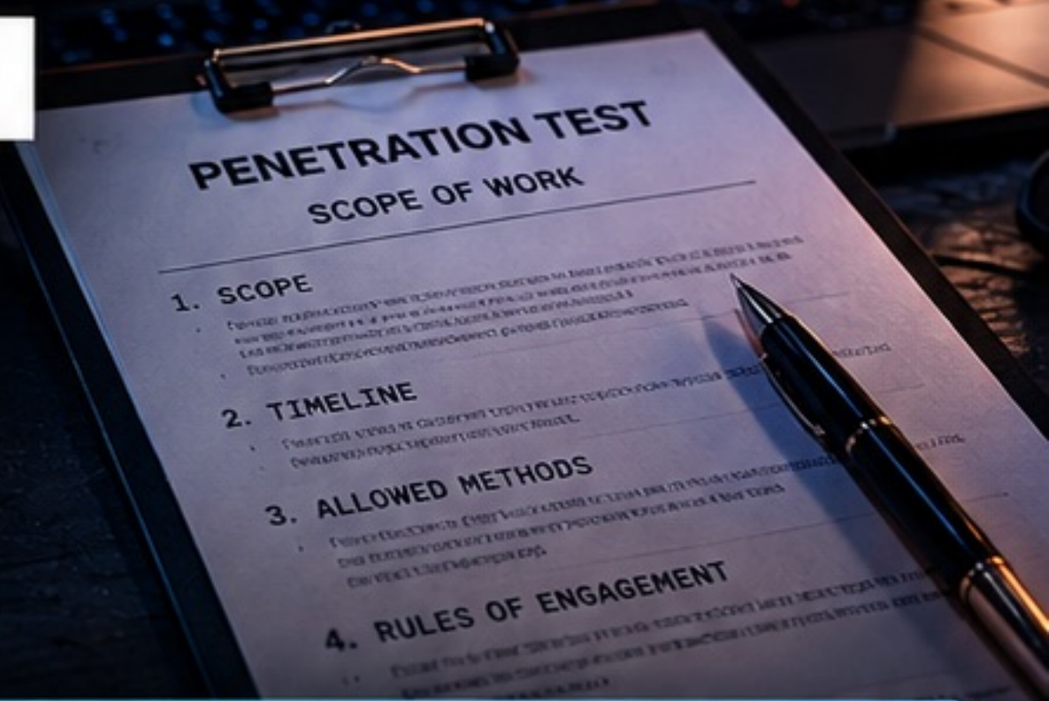
→ FINAL REPORT



Это не прямая линия: после отчёта клиент исправляет уязвимости, мы проводим повторное тестирование — и цикл начинается снова.

Документы до пакетов

Перед отправкой первого пакета всё должно быть согласовано на бумаге. Это может быть скучно, но именно это защищает вас.



ПРАВИЛА ВЗАИМОДЕЙСТВИЯ

ПОДПИСЫВАЮТСЯ ОБЕИМИ СТОРОНАМИ ПЕРЕД СТАРТОМ

1. **Scope**
   Какие системы, приложения и сети входят в тест, а какие — нет.
2. **Timeline**
   Окно тестирования: даты, время и что происходит, если продакшен недоступен.
3. **Allowed methods**
   Разрешённые техники: допустим ли social engineering, Denial of Service, физический доступ? Всё прописывается.
4. **Emergency contact**
   Кто на связи 24/7, если что-то пойдёт не так. Контакты с обеих сторон.
5. **Legal authorization**
   Подписанное разрешение от владельца систем. Без него тест не начинается.

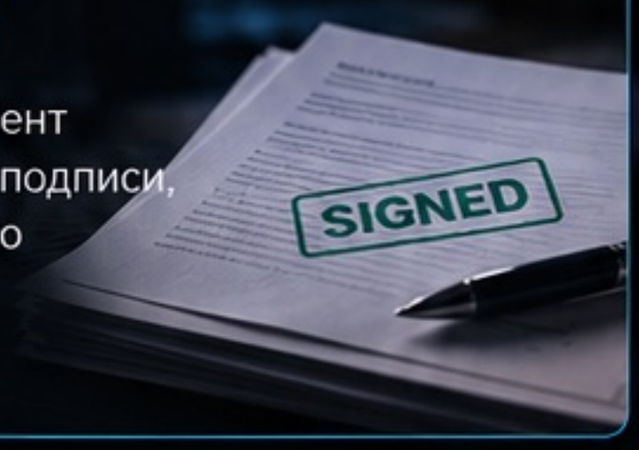
ПОЧЕМУ ЭТО ВАЖНО

Одна система за пределами scope — и ваш тест может стать несанкционированным доступом. Подписанный договор — это ваша правовая защита.



РЕЗУЛЬТАТ

Подписанный документ без “серых зон”. Ни подписи, ни скана, ни простого сообщения — этого недостаточно.



ТЕРМИН: SCOPE

Чёткий список того, что вам разрешено тестировать. Всё, что не указано в scope, считается запрещённым.



01 Kickoff call → 02 Обсуждение scope → 03 Контракт + подпись (RoE) → 04 Старт тестирования

ГЛАВНОЕ ПРАВИЛО Без письменного разрешения — нет теста.
Несанкционированное тестирование является преступлением почти во всех странах, даже при благих намерениях.

ФАЗА 02 · РАЗВЕДКА (RECONNAISSANCE)

Знай, прежде чем касаться

Можно узнать очень многое о цели, даже не взаимодействуя с ней. И большая часть нужной информации уже публична.



ПУБЛИЧНЫЕ ИСТОЧНИКИ · НУЛЕВОЙ КОНТАКТ С ЦЕЛЬЮ

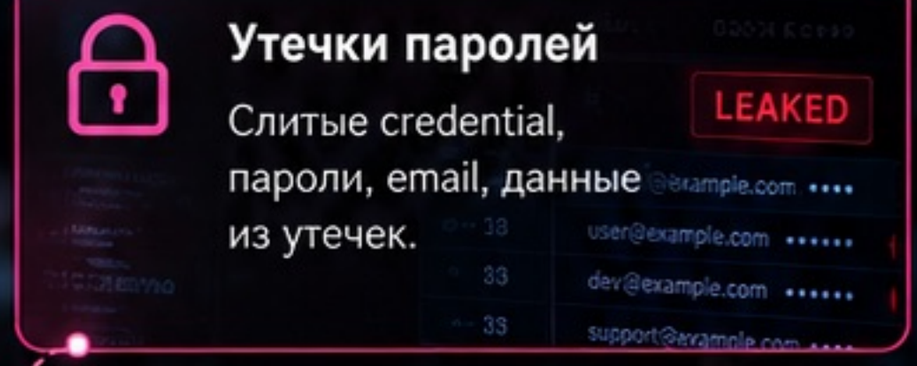
Домены и DNS

Информация о доменах, DNS-записях, поддоменах, IP-адресах.



Утечки паролей

Слитые credential, пароли, email, данные из утечек.



Вакансии (технологический стек)

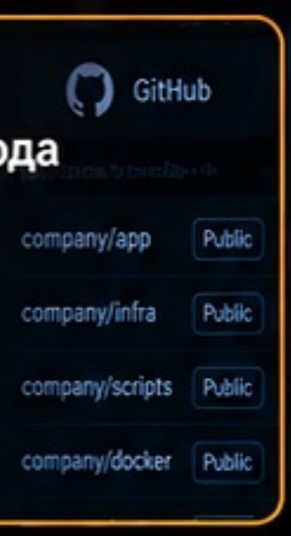
Публикации о работе показывают используемые технологии, инструменты и внутренние процессы.



ЦЕЛЬ

Публичные репозитории кода

Исходный код, конфиги, комментарии и история коммитов могут раскрыть архитектуру и уязвимости.



Социальные сети сотрудников

Профили сотрудников, их роли, контакты, информация о проектах и возможных точках входа.



Архивные версии сайтов

Старые версии сайтов могут содержать удалённые данные, скрытые файлы и интересные находки.



Пассивная разведка (Passive Recon)

Вы не взаимодействуете с их системами. Используете поисковые системы, публичные источники и утечки. Цель этого не видит.

Активная разведка (Active Recon)

Вы взаимодействуете: заходите на сайт, запрашиваете DNS, сканируете ресурсы. Это может отразиться в их логах.

OSINT — это законно Open Source Intelligence. Информацию может найти любой — публично и легально, без взлома и получения доступа.

Проверь каждую дверь

Разведка уже подсказала, где находится цель.
Теперь проверяем, какие двери открыты
и кто на них отвечает.



РЕЗУЛЬТАТ СКАНИРОВАНИЯ ПОРТОВ (ОДИН ХОСТ)

3 ОТКРЫТЫ · 1 ЗАКРЫТ · 1 ОТФИЛЬТРОВАН

22 SSH



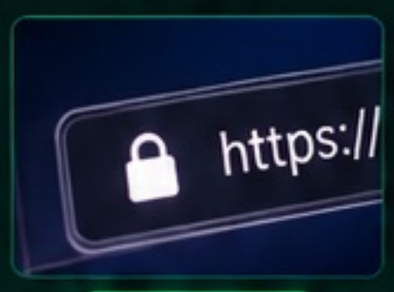
ОТКРЫТ

80 HTTP



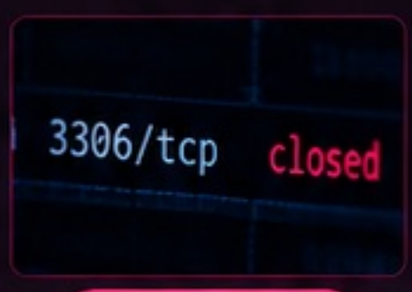
ОТКРЫТ

443 HTTPS



ОТКРЫТ

3306 DATABASE



ЗАКРЫТ

445 SMB



ОТФИЛЬТРОВАН

Открытый порт
Сервис отвечает.

Закрытый порт
Сервис недоступен.

Отфильтрованный порт
Заблокирован файрволом.

ДАЛЬШЕ — ПЕРЕЧИСЛЕНИЕ (ENUMERATION)

Для каждого открытого порта задаём правильные вопросы:

Какая версия ПО запущена?
Ищем известные уязвимости.

Какие учётные записи существуют?
Можно ли войти или перебрать?

Какие общие папки доступны?
Есть ли интересные файлы?

Какие функции включены?
Например, анонимный доступ, гостевые учётки, дополнительные модули.

Сканирование показывает двери. Перечисление — что за ними:
кто там живёт, какие данные доступны и что можно использовать на следующем этапе.

PORT Это номер, по которому компьютер принимает соединения.
У каждой машины **65 535** портов.

ФАЗА 04 · АНАЛИЗ УЯЗВИМОСТЕЙ

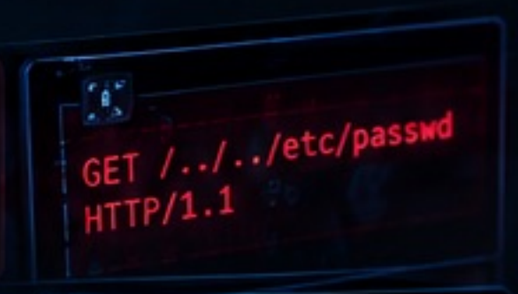
Что на самом деле сломано?

Сканирование дало список сервисов и версий.
Теперь сопоставляем каждую находку с известными уязвимостями и оцениваем, что действительно важно.



СОПОСТАВЛЕНИЕ ПРИМЕРОВ · ЧТО НАЙДЕНО → ЧТО ЭТО ЗНАЧИТ

Web server
устаревшая версия (2 года назад)
→ **Известная уязвимость** — Удалённое чтение файлов (path traversal) — CRITICAL



Форма входа
нет ограничений на попытки
→ **Известная уязвимость** — Подбор паролей (brute-force) — HIGH



Устаревшие настройки шифрования
→ **Известная уязвимость** — Трафик может быть расшифрован — MEDIUM

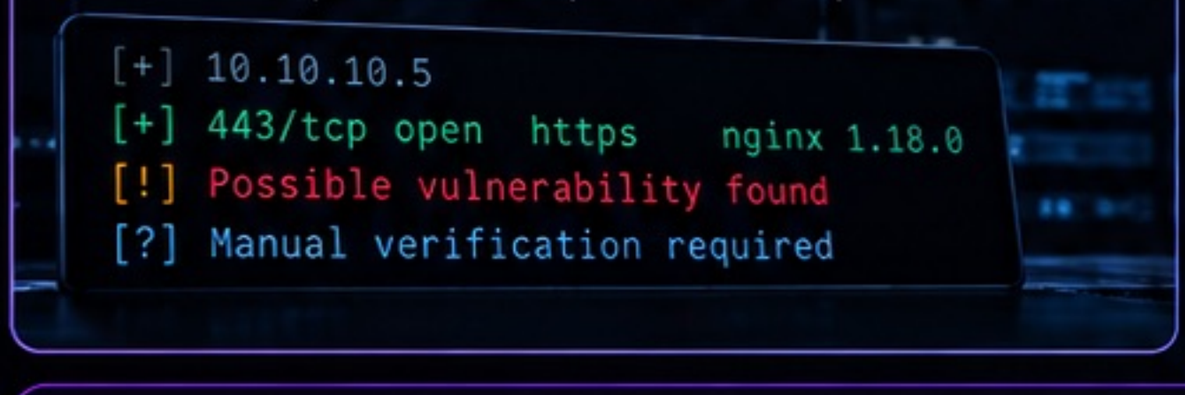


ШКАЛА КРИТИЧНОСТИ · КАК ПРИОРИТИЗИРУЕМ

CRITICAL	HIGH	MEDIUM	LOW	INFO
Исправлять немедленно	Исправить в ближайшее время	Запланировать исправление	Желательно исправить	Просто для информации

Сканеры не идеальны

Автоматические инструменты могут давать ложные срабатывания.
Всегда проверяйте находки вручную, прежде чем присваивать критичность.



Контекст определяет риск

Уязвимость с уровнем Medium в платёжной системе может быть опаснее, чем Critical на забытном тестовом сервере.

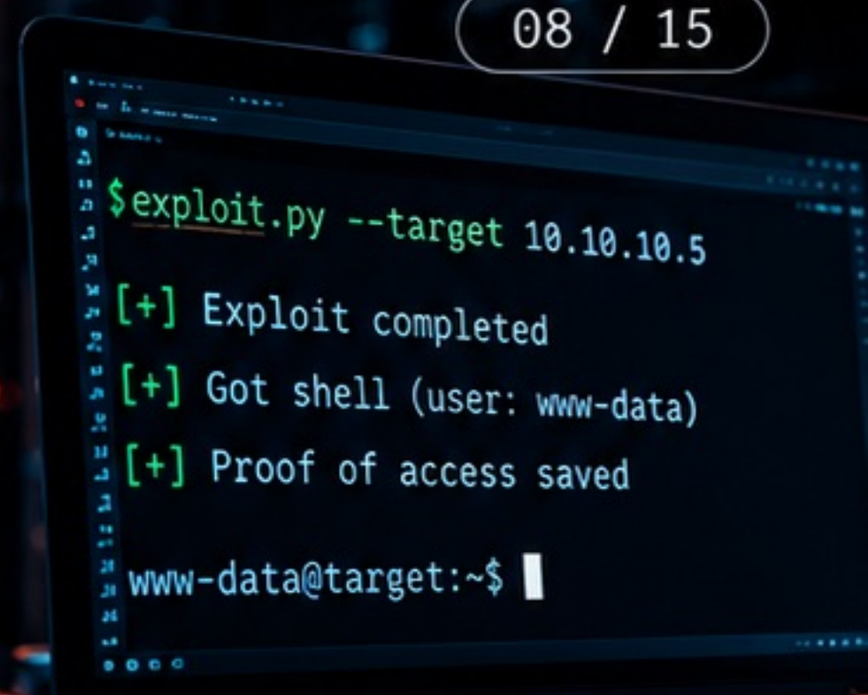


CVE — Common Vulnerabilities and Exposures — публичный идентификатор известной уязвимости. По нему можно найти подробную информацию: описание, примеры, патчи и рекомендации.

ФАЗА 05 · ЭКСПЛУАТАЦИЯ

Докажи это. Не ломай.

Теперь используем найденную уязвимость, чтобы получить доступ. Цель — подтвердить проблему, а не положить продакшен.



ОТ УЯЗВИМОСТИ К ДОСТУПУ

Уязвимость
Проблема, подтверждённая на предыдущем этапе

Эксплуатация
Код или действия, которые используют уязвимость

Первый доступ
Попадаем внутрь системы

КАК ЭТО ДЕЛАЕТ ПРОФЕССИОНАЛ

1

Выбираем безопасный путь

Используем read-only подход, где это возможно. Избегаем действий, которые могут повлиять на сервис.



2

Тестируем вне продакшена

По возможности используем лабораторную копию, staging или согласованное окно (off-hours).



3

Фиксируем доказательства

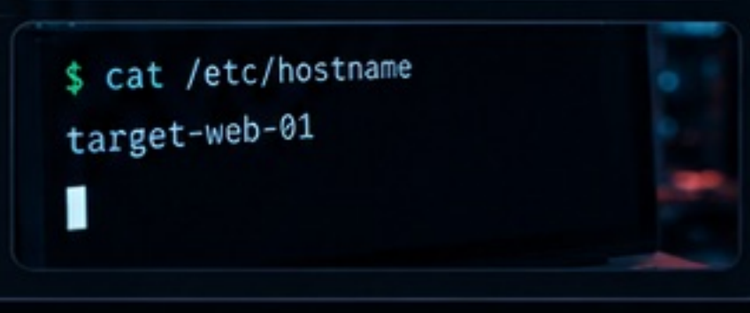
Делаем скриншот, сохраняем файл, фиксируем артефакт — любое безопасное подтверждение доступа.



4

Останавливаемся на согласованном уровне

В рамках scope показываем, что доступ получен. Не трогаем данные клиента и не идём дальше.



Падение сервиса во время pentest — это провал.

Эксплуатация — это хивургия, а не разрушение. Мы доказываем уязвимость, а не ломаем инфраструктуру.



Proof of Concept (PoC)

Минимальное, но достаточное подтверждение того, что уязвимость реально эксплуатируется. Например: вывод текущего пользователя, чтение файла или доступ к ограниченному ресурсу.



ФАЗА 06 · ПОСТЭКСПЛУАТАЦИЯ

И что дальше? Оцениваем влияние.



Первый доступ — это только начало.
Здесь мы отвечаем на главный вопрос:
насколько серьёзными могут быть последствия?

ОТ ПЕРВОЙ ТОЧКИ ДО ПОЛНОГО ВЛИЯНИЯ

КАЖДЫЙ ШАГ ПРОВЕРЯЕМ И ФИКСИРУЕМ

Первая точка
Компрометация одного низко-привилегированного аккаунта.

Больше прав
Повышение привилегий do **admin**-уровня.

Больше систем
Движение по инфраструктуре и доступ к другим машинам.

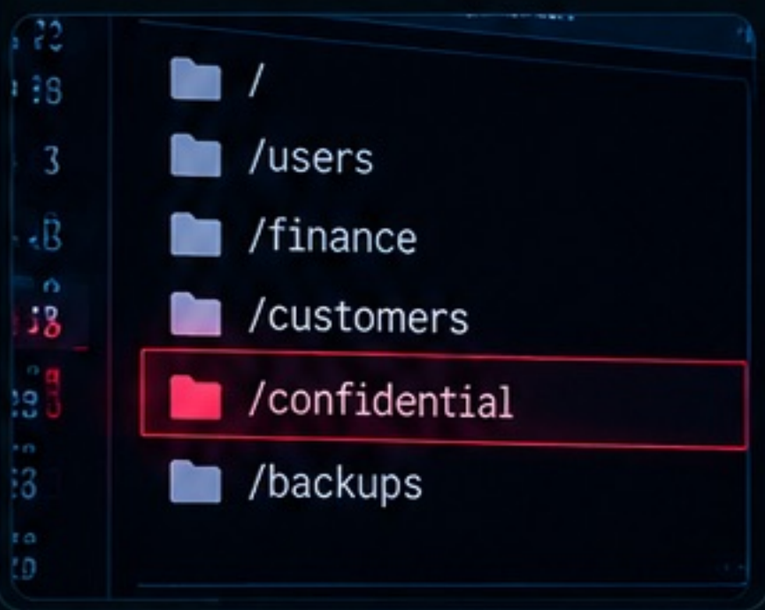
Критические данные
Доступ к тому, что принесёт наибольший ущерб бизнесу.

ЧТО РЕАЛНО ПОКАЗЫВАЕТ ЭТА ФАЗА

Охват
Насколько далеко можно продвинуться от одной уязвимости.



Чувствительные данные
Какие данные оказываются в зоне доступа.



Обнаружение
Замечают ли защитники наши действия.



Lateral Movement — Переход с одной скомпрометированной машины на другие, чтобы понять реальный масштаб возможного ущерба.

ФАЗА 07 · ОТЧЁТ (REPORTING)

Реальный результат

Находки сами по себе ничего не исправляют. Отчёт — это то, за что клиент действительно платит, и самая сложная часть работы.



ЧТО ВХОДИТ В ОТЧЁТ

CONFIDENTIAL

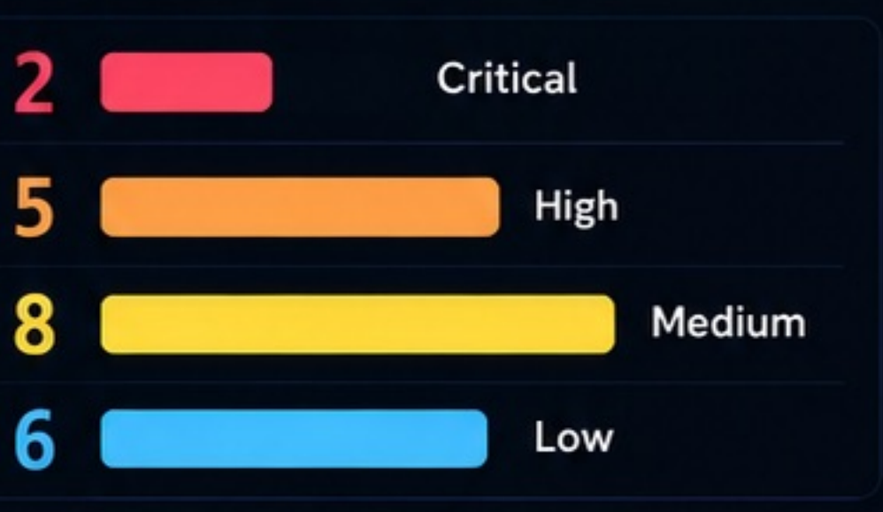
Краткое резюме (Executive Summary)
Одна страница, без лишнего, для руководства.

Находки с оценкой критичности
Каждая уязвимость с доказательствами и понятными шагами воспроизведения.

Рекомендации по устранению
Как исправить каждую проблему, в порядке приоритета.

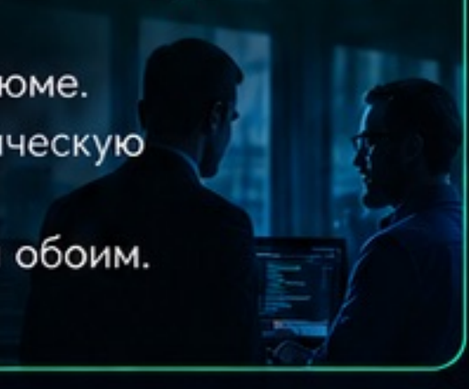
Техническое приложение
Детальные логи, команды, PoC, скриншоты и дополнительные данные для инженеров.

НАХОДКИ ПО УРОВНЮ КРИТИЧНОСТИ



ДВЕ АУДИТОРИИ — ОДИН ОТЧЁТ

Руководство читает резюме.
Инженеры читают техническую часть.
Хороший отчёт полезен обоим.



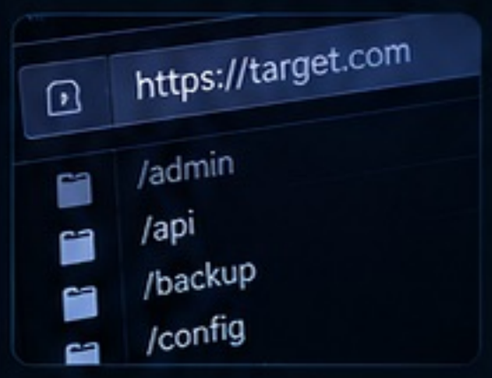
КАЖДАЯ НАХОДКА ОТВЕЧАЕТ НА ЧЕТЫРЕ ВОПРОСА

1 ЧТО?
В чём уязвимость.



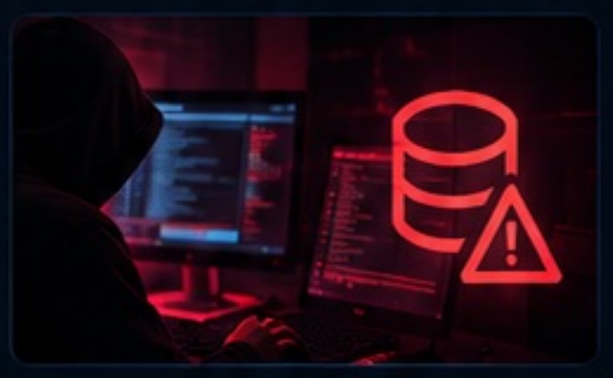
Например: возможность brute-force для логина.

2 ГДЕ?
Где она найдена.



URL, сервис, версия, конфигурация.

3 КАКОЕ ВЛИЯНИЕ?
Чем это опасно в реальности.



Например: несанкционированный доступ к данным клиентов.

4 ЧТО ДЕЛАТЬ?
Как это исправить.



Пошаговые рекомендации с приоритетом.

ЦЕЛЬ | Показать реальный масштаб риска и дать понятный план исправления, чтобы уменьшить его.

ПОСЛЕ ОТЧЁТА

Это цикл, а не финиш

Пентест — это снимок системы во времени. Инфраструктура меняется, появляются новые уязвимости. Ценность приходит, когда закрываем цикл и тестируем снова.



ШАГ 1

Тестирование

Находим уязвимости

```
$ nmap -sV target
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
```

ШАГ 2

Отчёт

Передаём находки



ШАГ 3

Исправление

Клиент закрывает уязвимости

```
[+] Patch applied
[+] Configuration updated
[+] Service restarted
```

ШАГ 4

Повторное тестирование

Проверяем, что всё исправлено

```
Re-scan ...
No critical issues
Fix verified
Ready
```

ПОВТОРЯТЬ

каждые 6–12 месяцев

Зачем повторно тестировать?

Исправление может быть неполным или открыть новую уязвимость. Только re-test подтверждает, что риск действительно устранён.

Безопасность — это процесс

Один тест защищает вас сегодня. Регулярное тестирование помогает оставаться защищёнными по мере роста и изменений системы.

МИФЫ VS РЕАЛЬНОСТЬ

Куда на самом деле уходит время?

Новички представляют пентест как часы взлома. На практике «хакинг» — лишь небольшая часть работы. Основное время уходит на анализ, документирование и коммуникацию.

ПРИМЕРНОЕ РАСПРЕДЕЛЕНИЕ ВРЕМЕНИ

ЗНАЧЕНИЯ МОГУТ ОТЛИЧАТЬСЯ В ЗАВИСИМОСТИ ОТ ПРОЕКТА

Разведка и сканирование Изучаем цель, строим карту инфраструктуры	25%
Анализ уязвимостей Проверяем, что реально представляет риск	20%
Эксплуатация Непосредственная эксплуатация и получение доступа	15%
Постэксплуатация Закрепление, оценка влияния, доп. проверки	10%
Отчёт и коммуникация Документируем, формулируем рекомендации, обсуждаем с командой	30%

ГЛАВНЫЙ ВЫВОД

Отчёт важнее «взлома»

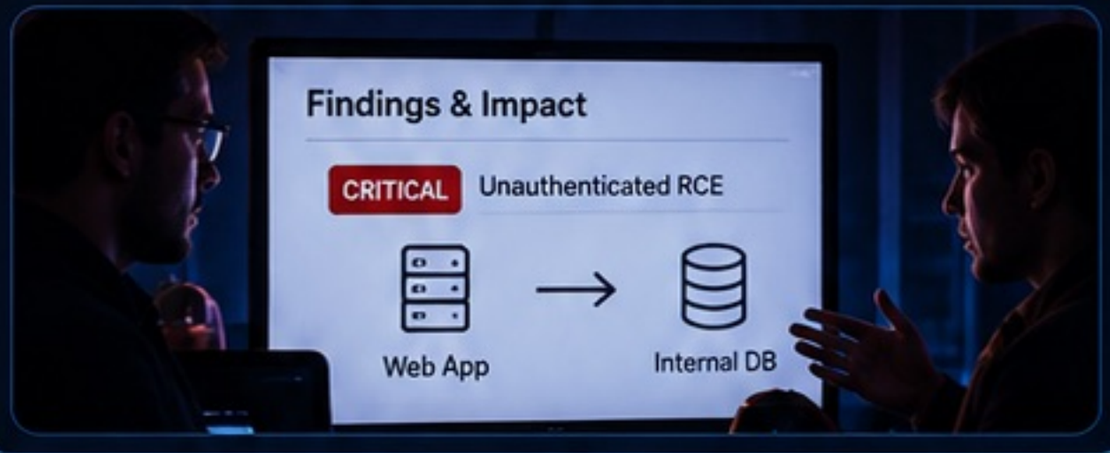
Ценность пентеста — не в самом доступе, а в качественном отчёте и понятных рекомендациях, которые действительно снижают риск.



ВАЖНЫЙ УРОК

Без коммуникации нет результата

Если вы не можете понятно описать находки и их последствия, вы не сможете быть эффективным пентестером.



Точные цифры зависят от цели, размера команды и scope.
Воспринимайте это как ориентировочную модель, а не жёсткое правило.

ПОЛЕЗНО ЗНАТЬ

Не все тесты одинаковые

Все 7 фаз остаются одинаковыми. Отличается лишь объём информации, которую получает тестировщик, и точка, с которой он начинает.

ТИПЫ ТЕСТИРОВАНИЯ ПО ОБЪЁМУ ЗНАНИЙ

Black Box

МИНИМУМ ИНФОРМАЦИИ

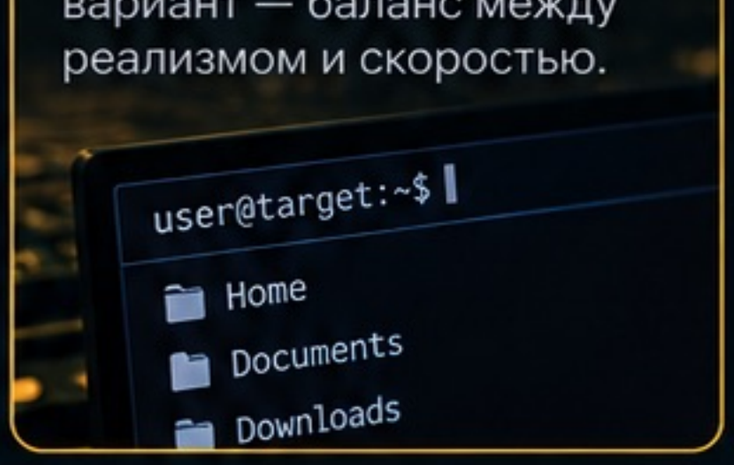
Вы ничего не знаете внутри. Видите только то, что доступно внешнему атакующему. Максимально приближено к реальной атаке, но идёт медленнее.



Gray Box

ЧАСТИЧНАЯ ИНФОРМАЦИЯ

Есть ограниченный доступ, например, учётная запись обычного пользователя. Самый распространённый вариант — баланс между реализмом и скоростью.



White Box

МАКСИМУМ ИНФОРМАЦИИ

Полный доступ к коду, документации и архитектуре. Позволяет найти максимум уязвимостей за меньшее время. Наиболее глубокое покрытие, но наименее похож на реальную атаку.

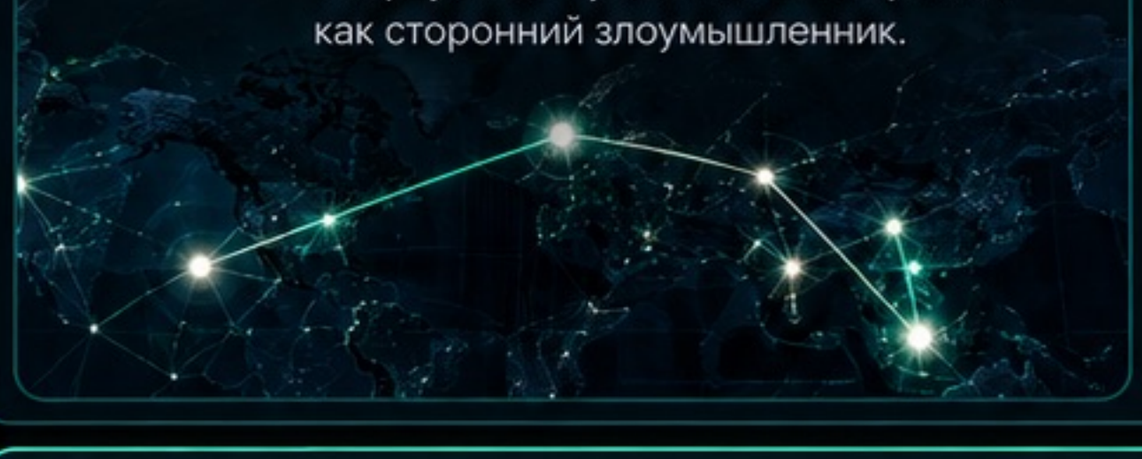


ОТКУДА ТЕСТИРОВЩИК НАЧИНАЕТ

External

КАК ВНЕШНИЙ АТАКУЮЩИЙ

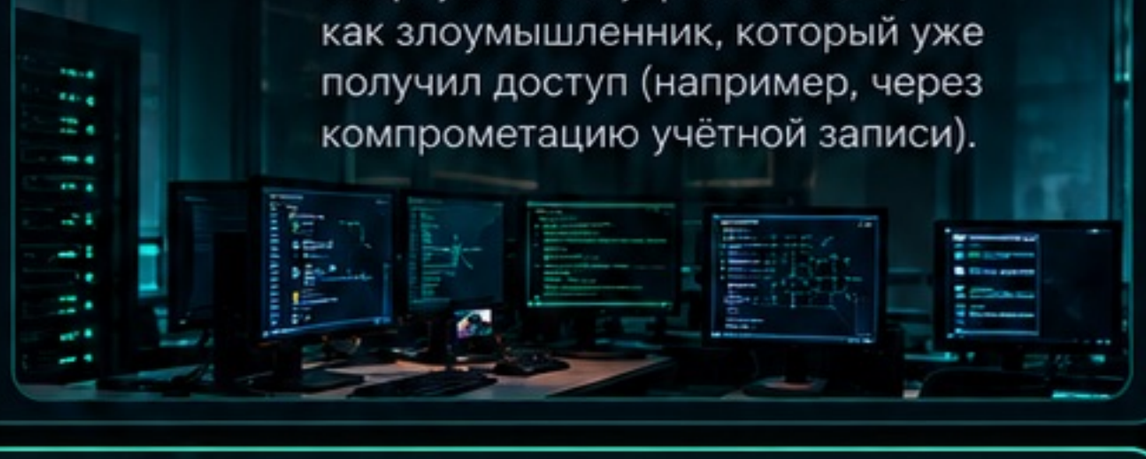
Стартуем из публичного интернета, как сторонний злоумышленник.



Internal

УЖЕ ВНУТРИ ИНФРАСТРУКТУРЫ

Стартуем из внутренней сети, как злоумышленник, который уже получил доступ (например, через компрометацию учётной записи).



Не существует «лучшего» типа теста. Всё зависит от того, на какой вопрос хочет получить ответ компания: уровень внешнего риска или глубина внутренних проблем.

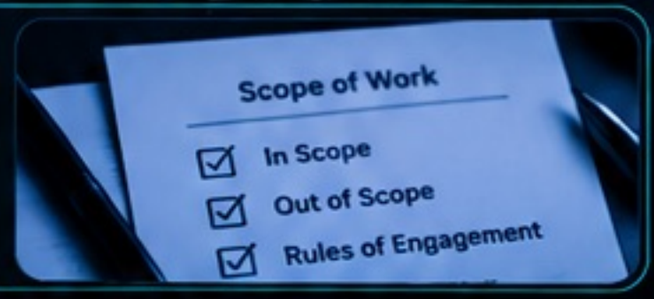
СОХРАНИ ЭТОТ СЛАЙД

7 фаз пентеста в одном взгляде



Весь процесс на одной карточке:
каждая фаза, её ключевая задача
и что она даёт для следующей.

1 **Подготовка к тестированию**
PRE-ENGAGEMENT
PERMISSION
Согласовываем scope и правила, фиксируем их в письменном виде.



2 **Разведка**
RECONNAISSANCE
PROFILE
Собираем публичные данные о цели: домены, технология, сотрудники, утечки.



3 **Сканирование и перечисление**
SCANNING & ENUM
PORTS
Находим открытые порты, запущенные сервисы и доступные функции.



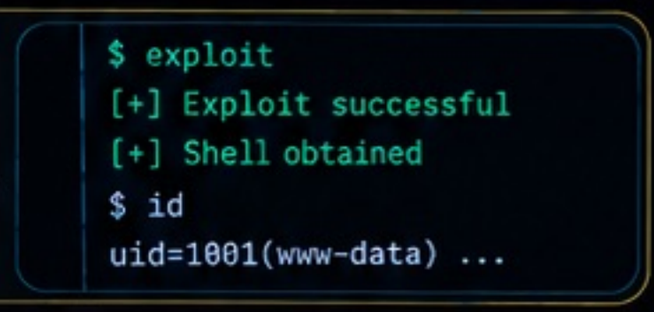
PORT	STATE	SERVICE
22/tcp	open	ssh
80/tcp	open	http
443/tcp	open	https
3306/tcp	open	mysql
8080/tcp	open	http-proxy

4 **Анализ уязвимостей**
VULN ANALYSIS
RANKED
Проверяем находки, подтверждаем уязвимости и расставляем приоритеты по риску.

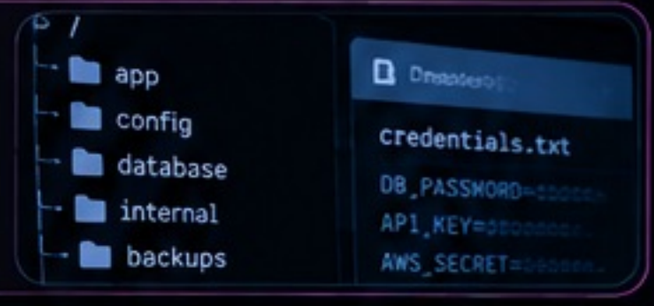


Vulnerability	Severity
SQL Injection	Critical
XSS	High
Open Redirect	Medium
Information Disclosure	Low

5 **Эксплуатация**
EXPLOITATION
PROOF
Используем уязвимость, получаем доступ и подтверждаем результат без нанесения ущерба.



6 **Постэксплуатация**
POST-EXPLOITATION
IMPACT
Оцениваем, как далеко можно зайти: масштабы доступа и реальное влияние на бизнес.



7 **Отчёт и рекомендации**
REPORTING
REPORT
Фиксируем все шаги, пишем понятные рекомендации, чтобы проблемы действительно исправили.



Сохрани этот слайд. **Это весь пентест-процесс в одном экране.**

@lionsoulbatyshchikov

Теперь ты знаешь, как работает пентест.

От подписанного scope до финального отчёта — все 7 фаз, через которые проходит каждый реальный пентест. Это больше, чем знают большинство.

Сохрани
ЧТОБЫ НЕ ПОТЕРЯТЬ

Это шпаргалка, к которой можно вернуться в любой момент.

Поделись
С КОЛЛЕГАМИ

Отправь тому, кто только начинает путь в кибербезопасности.

Подпишись
НОВЫЕ ГАЙДЫ КАЖДУЮ НЕДЕЛЮ

Практические материалы, разборы уязвимостей и советы из реальных пентестов.