

Рабочее окружение для
анализа
защищенности:
tips & tricks





Evgeny Stroev
Security Expert



Pentest

Большие и не очень компании, банки, заводы, паромы



Business Information Security

Изменение процессов, анализ рисков, практическая ИБ



Professional Consultation

Карьерные консультации, virtual-CISO, анализ защищенности



Career

Positive Technologies – Research & Development
AlfaBank – Security Operation Center & Red Team
Tinkoff – Business Information Security Officer
Exness – Security Business Analyst



Альфа-Банк



Путь самурая

- Бесплатный курс показывает карту - **широта**
- Workshop дает рабочую базу - **готовность с первого дня**
- Программа нарабатывает практику - **глубина и опыт**

Что будем делать



Рабочее окружение

Что это, из чего состоит, возможные варианты, нюансы



Настройка

Безопасность, удобство, эффективность



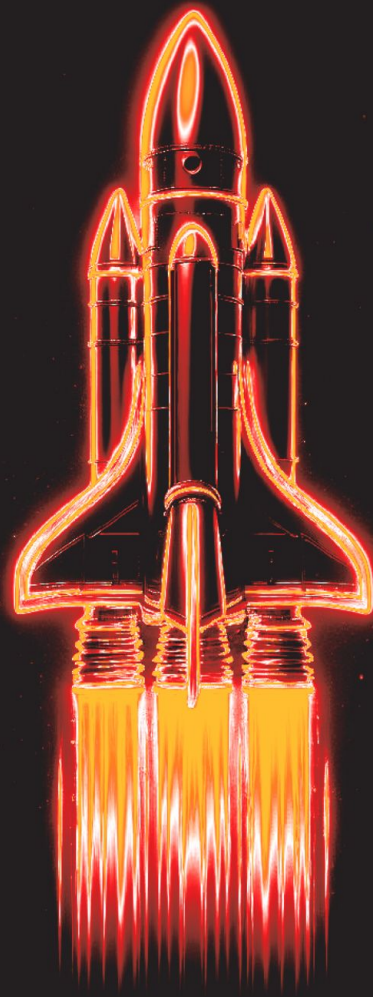
Использование

Инструменты, сервисы, нюансы



Вопросы & Ответы

Как жить дальше, что нам всем делать и есть ли в этом смысл



Рабочее окружение

Составляющие

- Платформа
- ОС
- Рабочее место
- Софт
- Интернет

Выбор платформы



Laptop



Desktop (PC)



VM



VPS (Cloud)



Mini-PC



Bare Metal

Платформа

Главный плюс

Главный минус

Laptop

Мобильность

Закрыл — все остановилось

PC

Мощность

Нет мобильности

VM

Откат и изоляция

Сетевые/USB нюансы

VPS

Автономность

Abuse / бан IP

mini-PC

Always-on дома

Ограниченные ресурсы

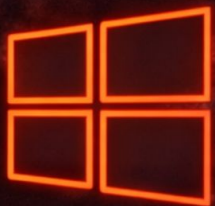
Bare Metal

Полный контроль

Сложно поддерживать

CyberED

Выбор ОС



Windows



macOS



Linux



Kali Linux

Выбор ОС

ОС	Главный плюс	Главный минус
Windows	Нужна для AD / PowerShell / native tooling	Не самая удобная базовая среда для offensive workflow
macOS	Удобна для повседневной работы	ARM и виртуализация могут создавать ограничения
Linux	Стандарт де-факто для offensive security	Некоторым новичкам сложнее как daily-driver
Kali Linux	Быстрый старт и готовая экосистема	Легко превратить в "мусорку из всего подряд"

Рабочее место: где вообще работает пентестер



Дома



В офисе



В кафе /
В метро / На улице



Из машины



Удаленно
(VPS / прокси / Tor)

CyberED

Рабочее ме

нтестер



Дома



Удаленно
(VPS / прокси / Tor)

Физический контекст и OPSEC

Рабочее место влияет не только на комфорт, но и на:

- Operations security (OPSEC) - операционная безопасность
- законность
- устойчивость связи
- наблюдаемость
- интерпретацию ваших действий окружающими

Физически

Рабочее место влияет

- OPSEC
- законность
- устойчивость с
- наблюдаемость
- интерпретацию



Физический контекст и OPSEC

- Домашняя сеть - не бесконечный ресурс;
- Корпоративная сеть работодателя - не место для “серых экспериментов”
- Публичные места создают лишний физический и юридический шум
- Чужие взломанные VPS использовать нельзя
- Tor - не магическая анонимность, а компромисс с медленностью, детектом и блокировками.

Физически

- Домашняя сеть
- Корпоративная
- Публичные мес
- Чужие взломан
- Tor - не магичес
- блокировками.



НТОВ”

ТЕКТОМ И

Интернет как часть окружения



Домашний
/ корпоративный



Мобильный



VPS

Интернет как часть окружения

Канал	Главный плюс	Главный минус
Домашний / корпоративный	Быстрый старт	IP / репутационные риски
Мобильный	Отдельный канал	Нестабильность / блокировки
VPS	Автономность	Abuse / ограничения хостера

CyberED

Софт



On-prem



Cloud



Open-source



Enterprise



Custom

CyberED

Софт

Тип софта	Главный плюс	Главный минус
Open-source	Лучший старт для обучения	Нужно самому разбираться, настраивать и поддерживать
Enterprise	Поддержка, стабильные процессы, командная работа	Дорого, не всегда доступно, иногда только под Windows
Custom	Можно точно закрыть свою рутину	Нужно писать, поддерживать и допиливать

Софт. Нюансы

Блок	Основные проблемы
Покупка и доступ	Дорого; ограничения продажи; санкции
Поддержка и стабильность	Нестабильность; поломки после обновлений; конфликты зависимостей; старые зависимости
Совместимость	Только Windows
Практика	Документация $\neq$ реальная жизнь
Порог входа	Нужно понимать принцип работы; иногда нужен код; сложно использовать

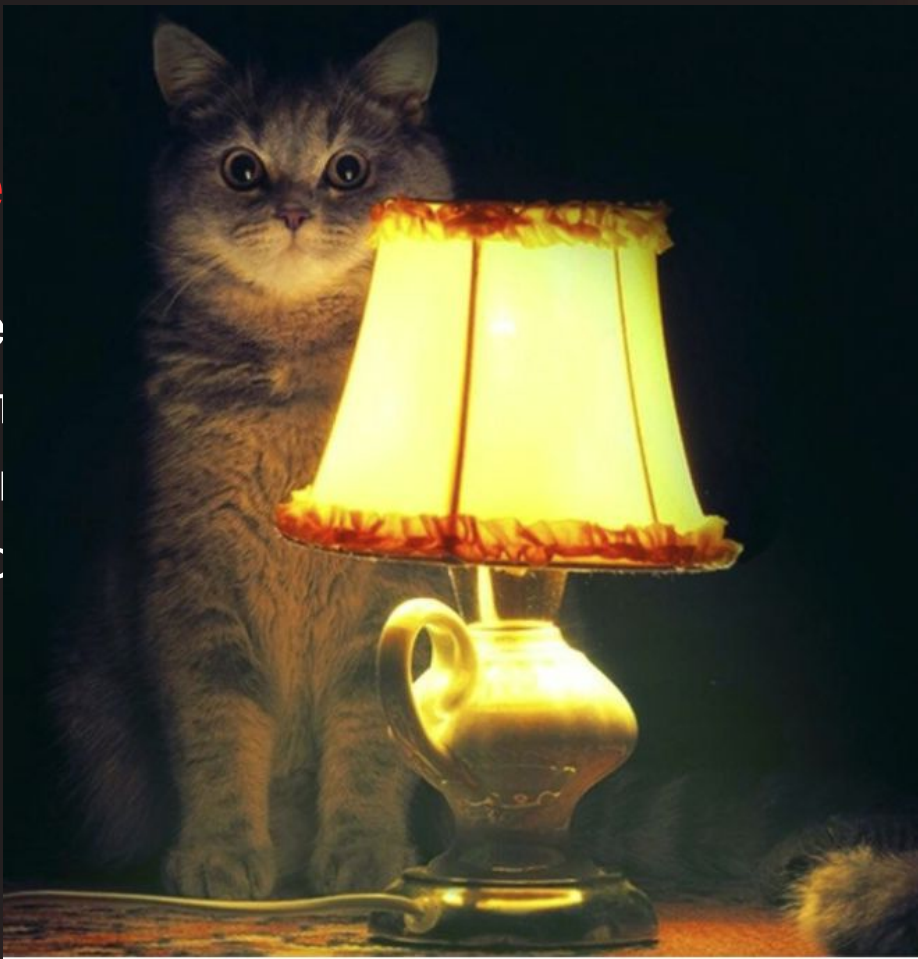
Почему не весь софт одинаково полезен

- Никому нельзя доверять
- Вы не контролируете бинарь
- Вас и ваши данные могут скомпрометировать
- Данные проекта могут скомпрометировать

Почему не

- Никому не
- Вы не конт
- Вас и ваш
- Данные пр

эзен



Когда писать свой инструмент

Когда	Главный плюс	Главный минус
Задача повторяется	Автоматизация экономит время	Нужно поддерживать код
Вход/выход стабилен	Можно стандартизировать workflow	Придется следить за изменениями форматов
Нужно склеить 2–3 инструмента	Удобный glue-layer	Легко написать хрупкий костыль
Вручную уже раздражает	Снимает рутину и ошибки	Можно переусложнить простую задачу
Нужен “свой птэр”	Почти нет реальной пользы	Потеря времени вместо практики
Задача случится один раз	Проще сделать руками	Автоматизация не окупится

Настройка

Основные моменты

- Hardening
- Инструменты
- Автоматизация
- Tips & Tricks

Настройка



[DEMO] Kali VM

Настройка



[DEMO] Debian VPS

- SSH + Hardening

Настройка



[DEMO] Удобство работы

- Рабочая структура
- Терминальная гигиена

Настройка



[DEMO] Базовые инструменты

- Python / pipx / uv
- Go

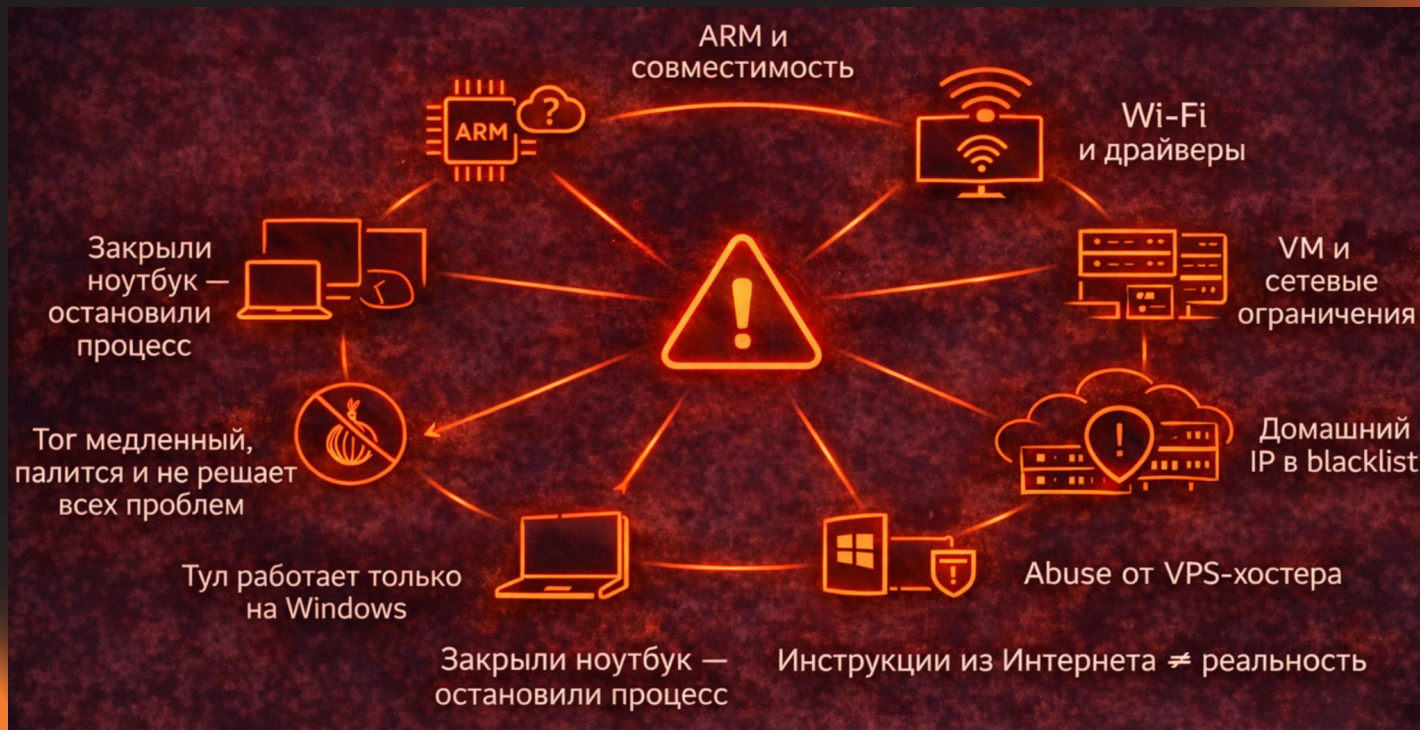
Настройка



[DEMO] Автоматизация

- Alias
- Function
- wrapper

Что чаще всего ломается на практике



Использование

Составляющие

- Профиль сканирования
- Spoofing/MITM/Bruteforce
- Запуск готовых скриптов с GitHub

Диаграмма зависимостей

Окружение как система, а не набор программ



Вопросы

Комментарии,
предложения, подарки

CyberED

Спасибо!

cyber-ed.ru

+7 (495) 181 00 79

info@cyber-ed.ru



VK



Telegram