5 проектов по кибербезопасности для старта

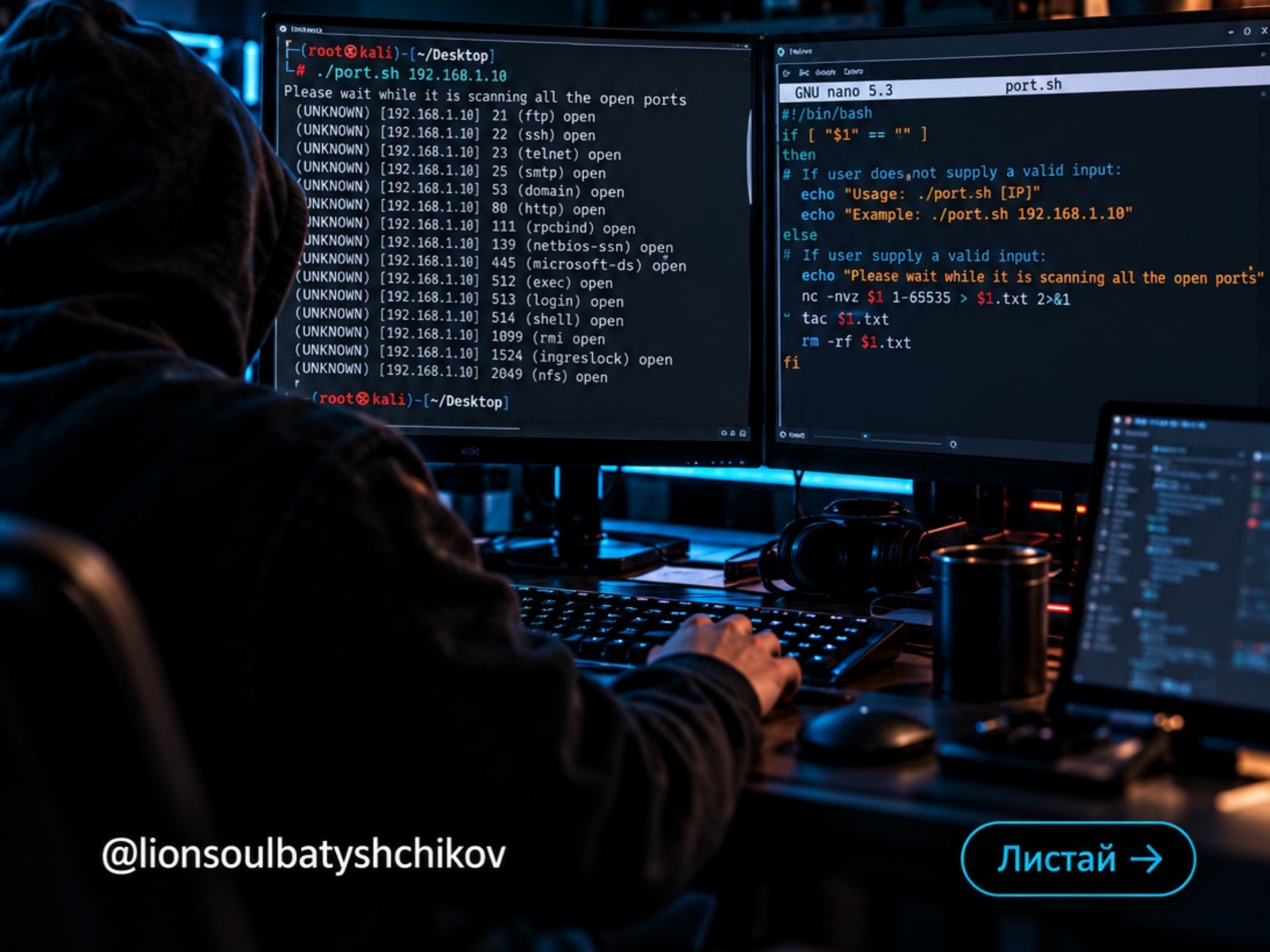
От теории к практике — собирай своё портфолио уже сегодня

@lionsoulbatyshchikov

Листай →

Почему стоит строить, а не просто смотреть

Просмотр уроков даёт мотивацию, но настоящий навык приходит только через практику. Собирай каждый проект в своём изолированном лабораторном окружении, фиксируй шаги и выводы. Готовый write-up — это уже часть твоего портфолио и реальный прогресс.

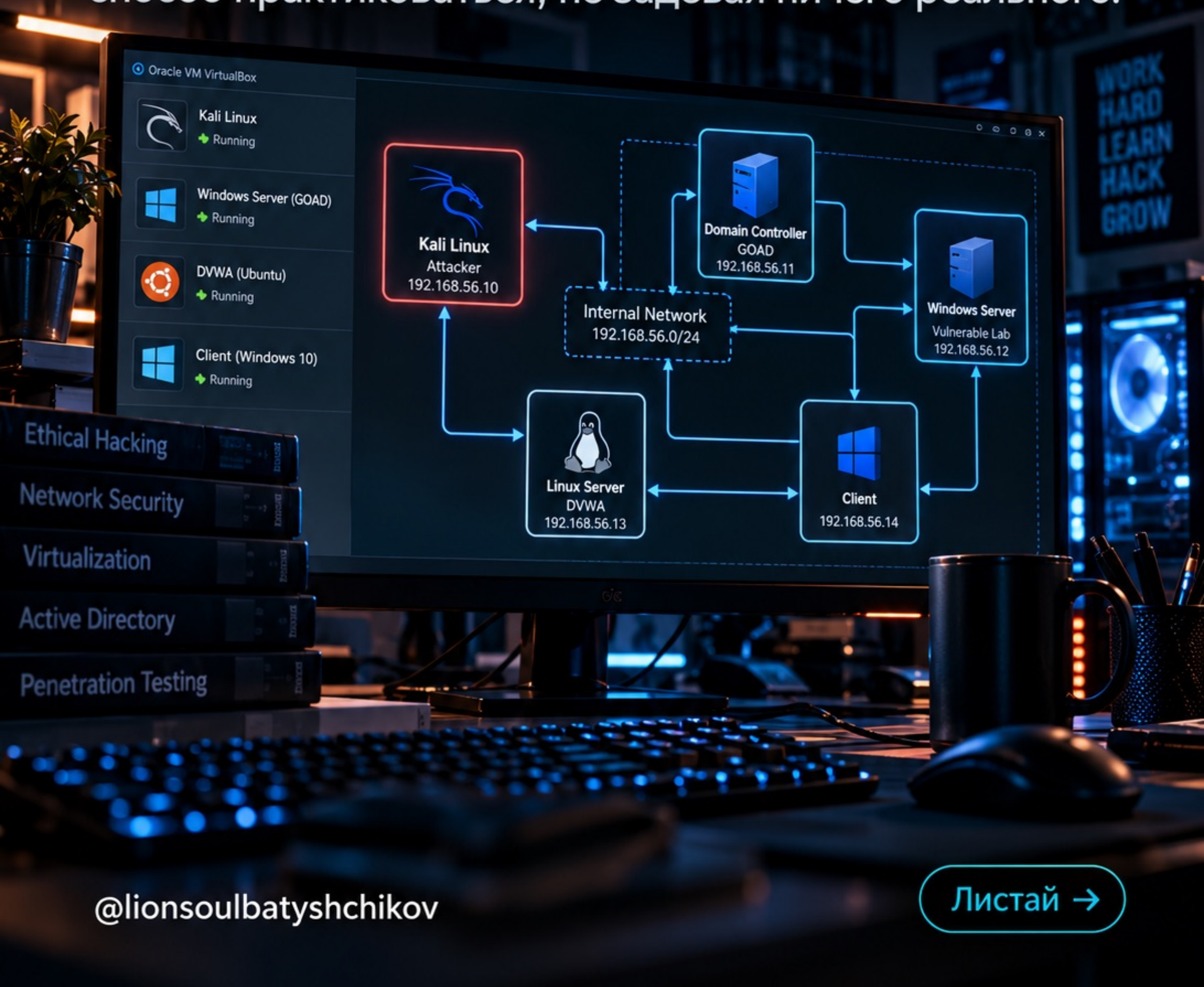


@lionsoulbatyshchikov

Листай →

Проект 1: свой лабораторный стенд дома

Собери изолированную сеть в **VirtualBox**: одна машина с **Kali** как атакующий и другая уязвимая (например, **GOAD** или **DVWA**) как цель. Это база для всех остальных проектов и безопасный способ практиковаться, не задевая ничего реального.

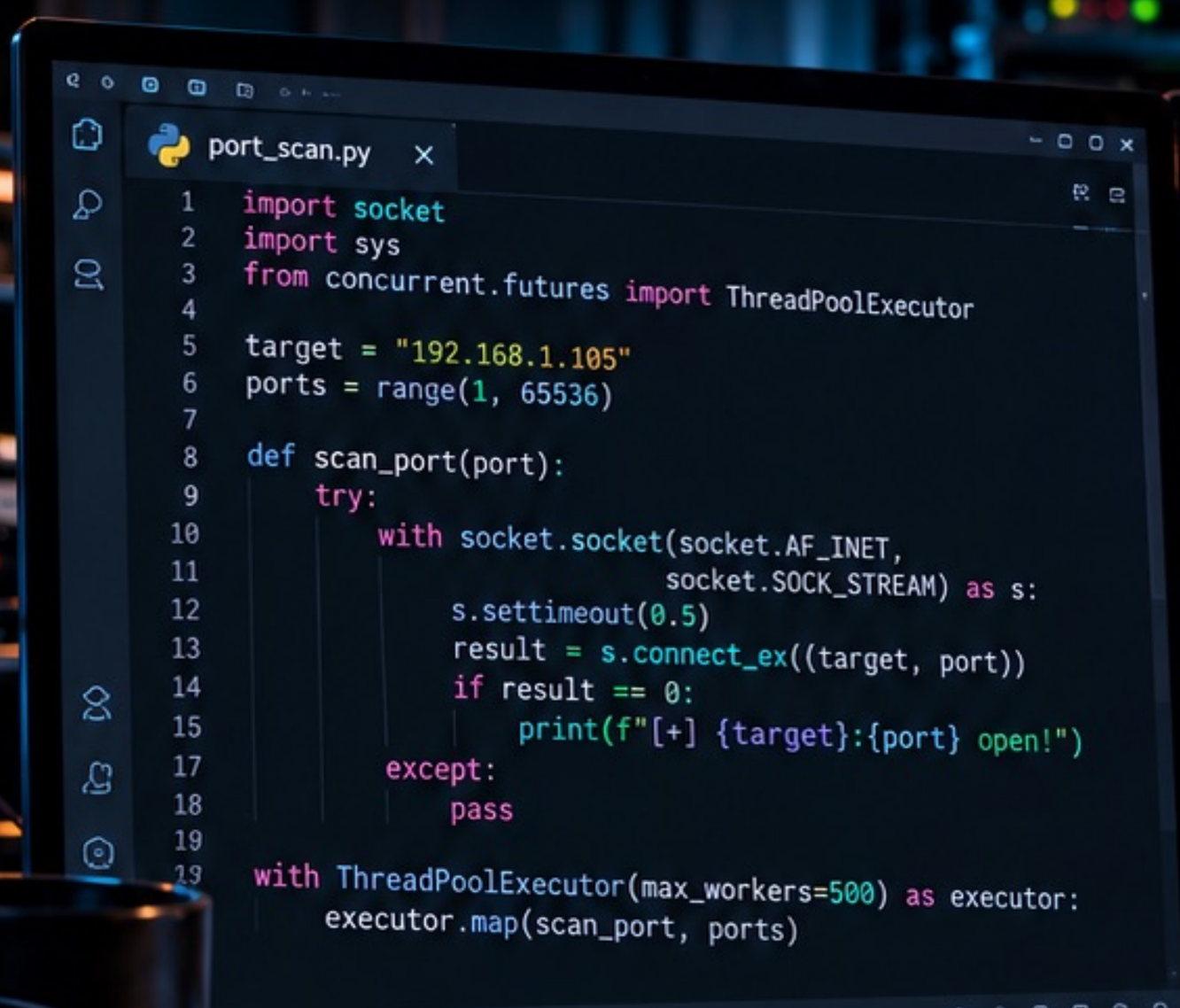


@lionsoulbatyshchikov

Листай →

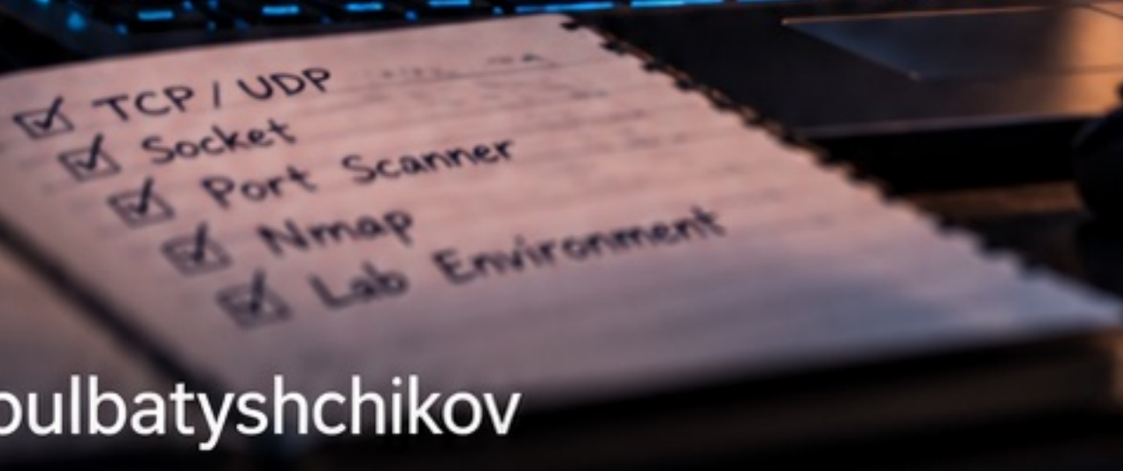
Проект 2: сканер портов на Python

С помощью модуля **socket** напиши сканер, который проверяет открытые порты на цели в твоей лаборатории. За несколько строк ты поймёшь, как работают **TCP**, сервисы и почему **Nmap** делает то, что делает. Тот же код, те же сети — отличная практика и реальный результат.







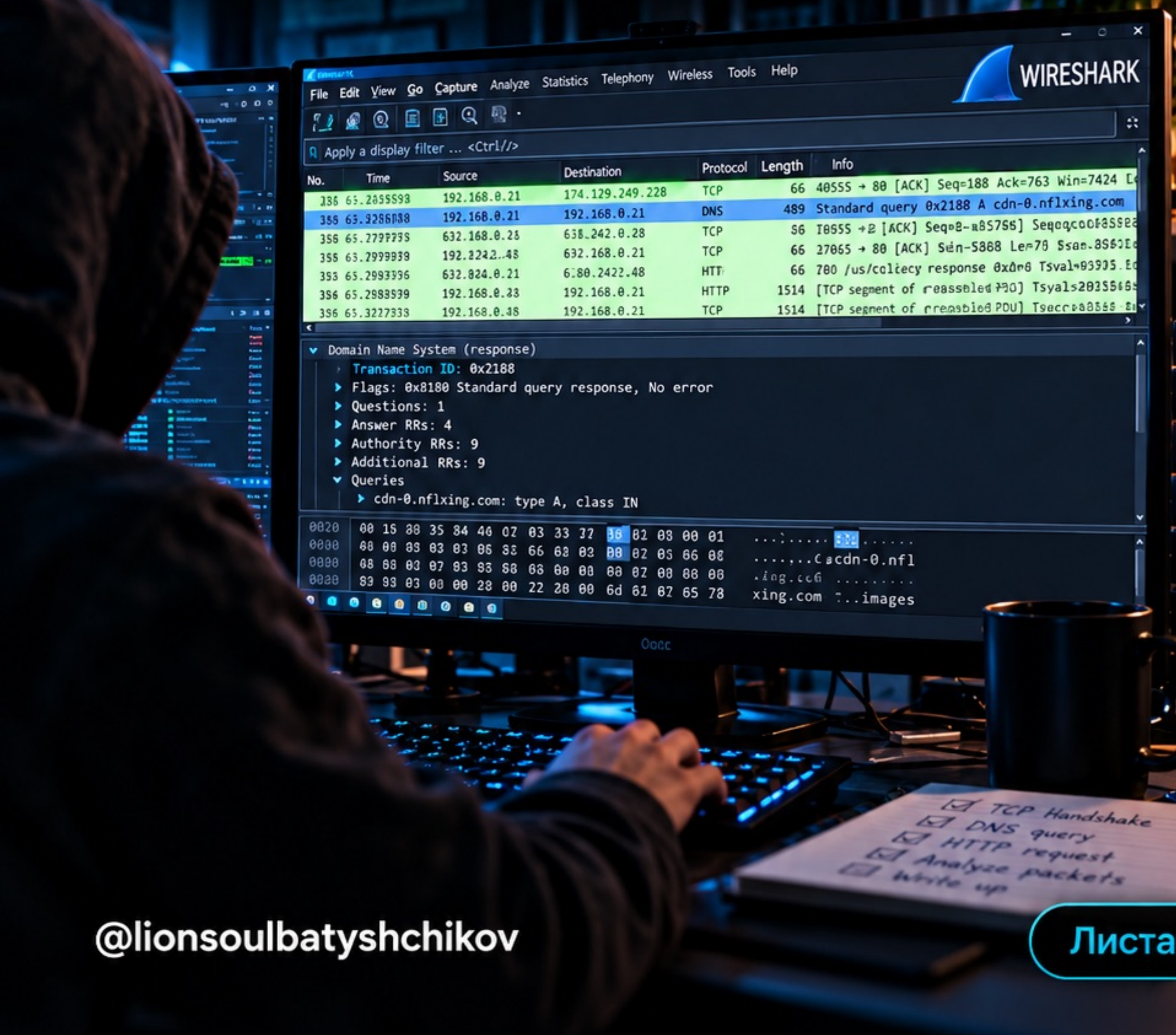


@lionsoulbatyshchikov

Листай →

Проект 3: анализ трафика в Wireshark

Захвати сетевой трафик в своей лаборатории и открой его в **Wireshark**. Найди **TCP handshake**, **DNS** запрос, **HTTP** login в открытом виде. Разберись, как выглядит реальный трафик в сети. Тот же дамп и тот же анализ — отличный навык и материал для **write-up**.



@lionsoulbatyshchikov

Листай →

Проект 4: проверка надёжности пароля

Напиши на **Python** скрипт, который проверяет длину, сложность и распространенные пароли. Для более продвинутой версии используй **Have I Been Pwned API** и проверяй, попадала ли пароли в утечки. Это отличный проект для отработки базового **scripting** и работы с реальными данными.

```
Windows PowerShell
PS C:\Projects\password-checker> python .\check_password_strength.py .\passwords.txt

[+] Проверка пароля: password
Длина: 8
Сложность: 0/4
Время взлома: меньше 1 секунды
Статус: найден в утечках (Have I Been Pwned)
Совет: используйте более длинный и уникальный пароль.

[+] Проверка пароля: 1234567
Длина: 7
Сложность: 0/4
Время взлома: меньше 1 секунды
Статус: найден в утечках (Have I Been Pwned)
Совет: используйте более длинный и уникальный пароль.

[+] Проверка пароля: S!opLabxtre_91TGCE
Длина: 20
Сложность: 4/4
Время взлома: столетия
Статус: не найден в утечках
Совет: надёжный пароль!

PS C:\Projects\password-checker>
```

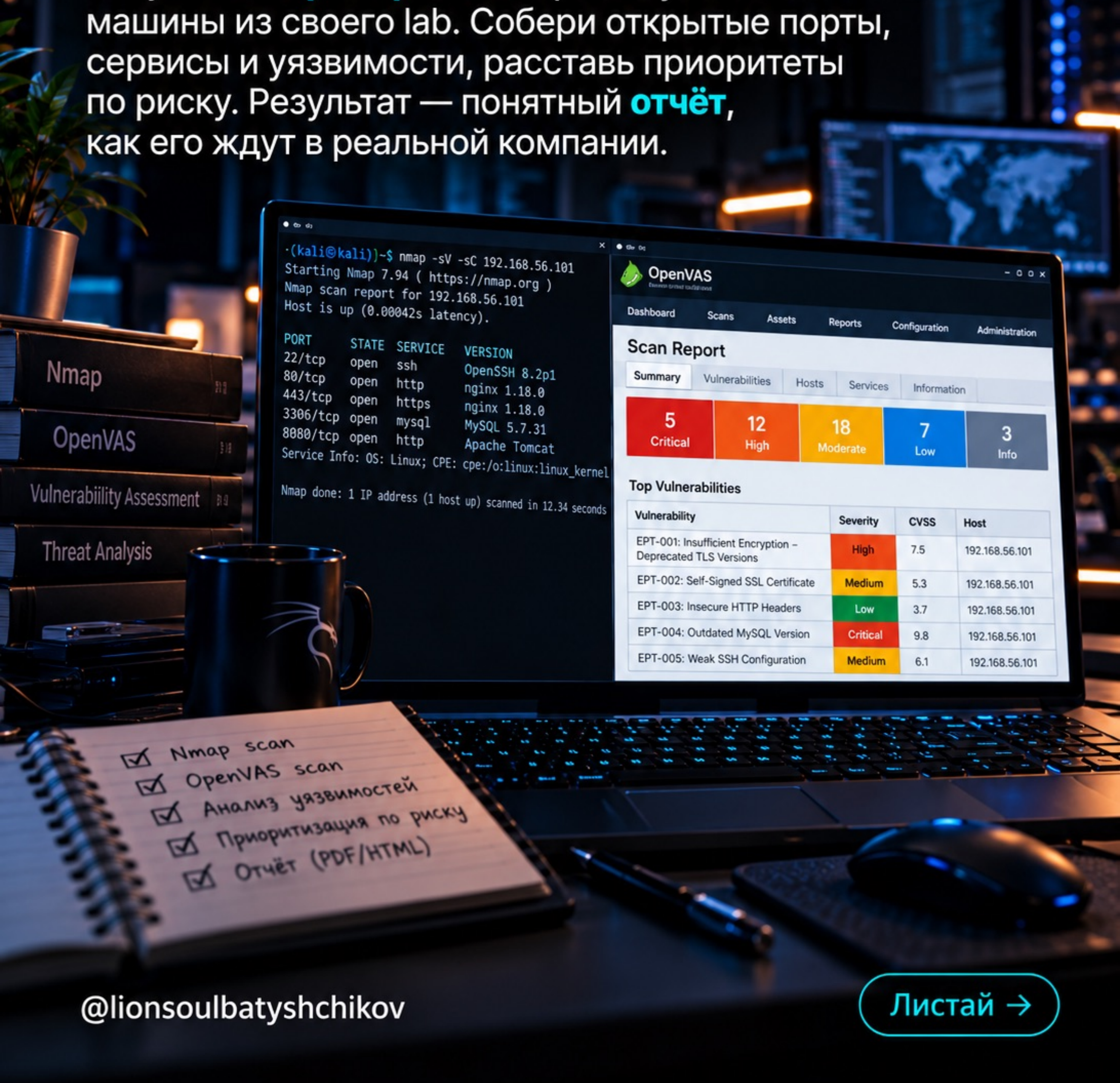
Password Checker
- Length check
- Character variety
- Common passwords
- Have I Been Pwned API
- Real data testing

@lionsoulbatyshchikov

Листай →

Проект 5: сканирование и отчёт по уязвимостям

Запусти **Nmap** и **OpenVAS** против уязвимой машины из своего lab. Собери открытые порты, сервисы и уязвимости, расставь приоритеты по риску. Результат — понятный **отчёт**, как его ждут в реальной компании.



@lionsoulbatyshchikov

Листай →