NMAP

ОТ ОСНОВ ДО ПРОДВИНУТОГО

30 ПРАКТИЧЕСКИХ ПРИМЕРОВ СКАНИРОВАНИЯ

```
nmap -sS -sV 192.168.1.0/24

PORT      STATE   SERVICE   VERSION
22/tcp    open    ssh       OpenSSH 9.6
80/tcp    open    http      nginx 1.24.0
443/tcp   open    https     nginx 1.24.0
3306/tcp  open    mysql     MySQL 8.0.33

Nmap done: 256 IP addresses
scanned in 42.67 seconds
```

```
nmap -A 10.10.10.0/24

PORT      STATE   SERVICE
21/tcp    open    ftp
22/tcp    open    ssh
80/tcp    open    http
443/tcp   open    https
3389/tcp  open    ms-wbt-server

Nmap done: 256 hosts up
scanned in 68.14 seconds
```

ИЗУЧАЙ
СИНТАКСИС И РЕЖИМЫ

АНАЛИЗИРУЙ
ХОСТЫ, ПОРТЫ, СЕРВИСЫ

ДОКУМЕНТИРУЙ
РЕЗУЛЬТАТЫ И НАХОДКИ

@lionsoulbatyshchikov

ЗНАЙ ЧТО ТЫ СКАНИРУЕШЬ

Обнаружение сети и аудит безопасности



ПОИСК ХОСТОВ

Находи активные системы в сети с помощью ping scan и техник обнаружения хостов.



ВИДИ ПОРТЫ

Определяй, какие TCP/UDP порты открыты, закрыты или отфильтрованы на каждом хосте.



ИЗУЧАЙ СЕРВИСЫ

Определяй запущенные сервисы, их версии и операционные системы для лучшей видимости.

Используй **Nmap** только на системах, которые тебе принадлежат или на которые у тебя есть разрешение.

@lionsoulbatyshchikov

УСТАНОВИ И ПОДГОТОВЬ NMAP

WINDOWS

1. Скачай установщик с официального сайта **nmap.org/download.html**
2. Установи Npcap, когда будет предложено.

DEBIAN / UBUNTU / KALI

```
$ sudo apt update
$ sudo apt install nmap
```

macOS

С установленным Homebrew:

```
$ brew install nmap
```

ПРОВЕРЬ УСТАНОВКУ

```
$ nmap --version
```

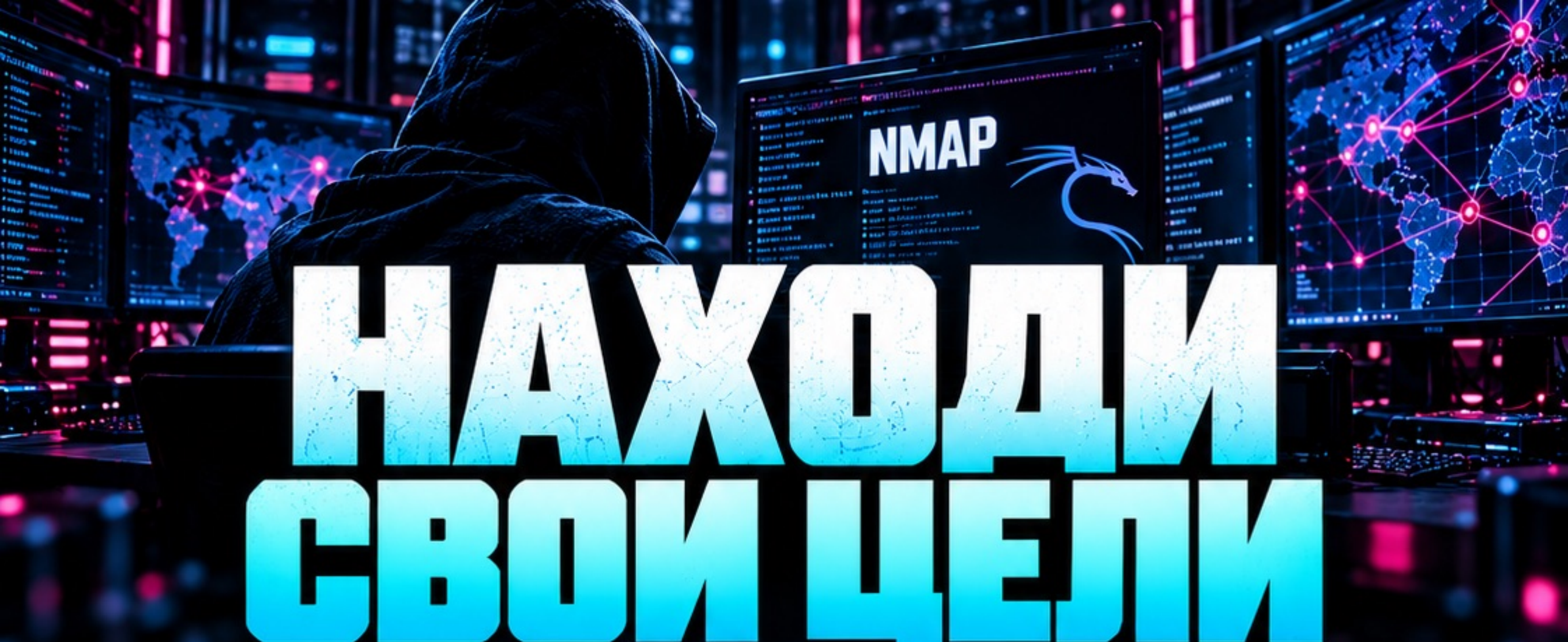
Пример: используй тестовый хост **192.168.1.10**

Замени его на свой разрешённый target.

Для Linux/macOS команды выполняются через sudo.

В Windows может потребоваться запуск от имени администратора.

@lionsoulbatyshchikov



НАХОДИ СВОИ ЦЕЛИ

01–05 / 30 ПРИМЕРОВ СКАНИРОВАНИЯ

01

$ **nmap 192.168.1.10**

Сканирует стандартные 1,000 TCP портов на указанном хосте.



02

$ **nmap 192.168.1.10 192.168.1.20**

Сканирует два хоста.



03

$ **nmap 192.168.1.1-20**

Сканирует диапазон IP-адресов.



04

$ **nmap -sn 192.168.1.0/24**

Находит активные хосты в подсети без сканирования портов.



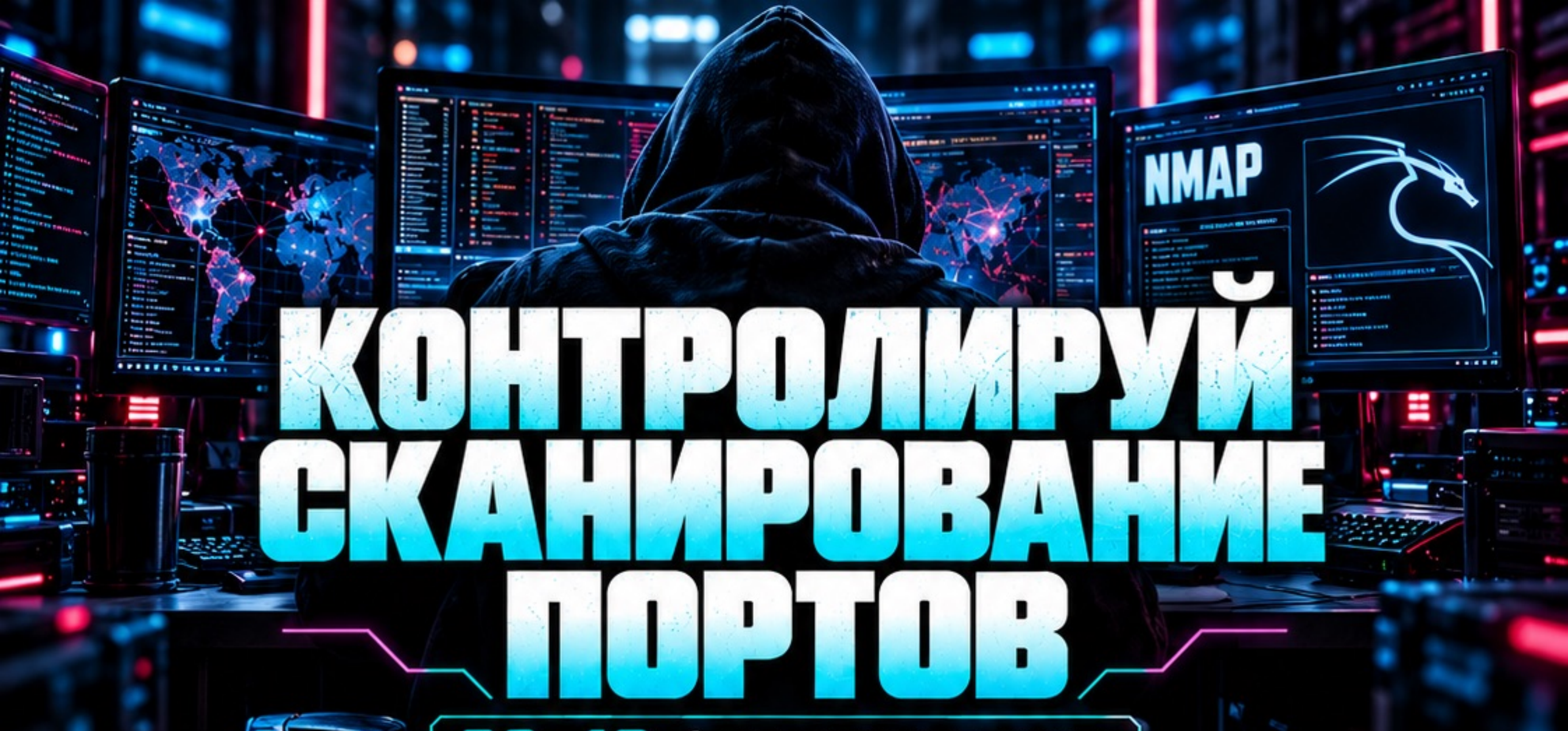
05

$ **nmap -sL -n 192.168.1.0/24**

Показывает список целей (IP-адресов) без сканирования и DNS-запросов.



Хост может быть активен, даже если он не отвечает на сканирование.



КОНТРОЛИРУЙ СКАНИРОВАНИЕ ПОРТОВ

06–10 / 30 ПРИМЕРОВ NMAP

06

```
$ nmap -p 22,80,443 192.168.1.10
```

Проверяет конкретные TCP порты на указанном хосте.

```
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
```

07

```
$ nmap -p- 192.168.1.10
```

Сканирует все TCP порты (1–65535) на хосте.

```
Scanning 1-65535 ports...
100.0%
65535 ports scanned
```

08

```
$ nmap --top-ports 100 192.168.1.10
```

Сканирует 100 самых популярных TCP портов.

```
Top 100 ports:
22/tcp    open    ssh
80/tcp    open    http
443/tcp   open    https
3306/tcp  open    mysql
```

09

```
$ nmap -sT 192.168.1.10
```

Использует полное TCP соединение (TCP connect scan).

```
Nmap scan report for 192.168.1.10
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   open     https
```

10

```
$ sudo nmap -sS 192.168.1.10
```

Использует TCP SYN сканирование (требуются root/добавочные privileges).

```
[SYN] ──► [SYN/ACK]
  └─► [RST]
```

ⓘ SYN сканирование всё ещё может быть обнаружено и записано в логи.



ОПРЕДЕЛЯЙ СЕРВИСЫ И СИСТЕМЫ

11–15 / 30 ПРИМЕРОВ NMAP

11

```
$ nmap -sV 192.168.1.10
```

Определяет названия сервисов и их версии.

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 9.2p1
80/tcp	open	http	nginx 1.24.0
443/tcp	open	https	Apache 2.4.58



12

```
$ nmap -sV --version-all 192.168.1.10
```

Пытается определить все возможные версии сервисов (более детальный анализ).

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 9.2p1
80/tcp	open	http	nginx 1.24.0
443/tcp	open	https	Apache 2.4.58
3306/tcp	open	mysql	MySQL 8.0.36

13

```
$ sudo nmap -O 192.168.1.10
```

Определяет операционную систему цели (OS detection).

```
Nmap scan report for 192.168.1.10
Host is up (0.0021s latency).
OS details: Linux 5.15 - 6.1
Network Distance: 1 hop
```



14

```
$ sudo nmap -A 192.168.1.10
```

Комплексное сканирование: определение ОС, версий сервисов, запуск скриптов и трассировка маршрута.

- OS detection
- Version detection
- Nmap scripts (default)
- Traceroute



15

```
$ sudo nmap -sU -p 53,123,161 192.168.1.10
```

Проверяет выбранные UDP сервисы и их состояние.

PORT	STATE	SERVICE
53/udp	open|filtered	domain
123/udp	open|filtered	ntp
161/udp	open|filtered	snmp



ⓘ Определение ОС — это предположение. UDP порты могут быть в статусе open|filtered.

@lionsoulbatyshchikov



ИССЛЕДУЙ С ПОМОЩЬЮ NSE SCRIPTS

16–20 / 30 ПРИМЕРОВ NMAP

16

$ **nmap -p 80,443 --script http-title 192.168.1.10**

Получает заголовки веб-страниц (http-title).

```
http://192.168.1.10
<title>Welcome to nginx</title>
<title>Apache2 Ubuntu Default Page</title>
<title>Login - Portal</title>
```

17

$ **nmap -p 80,443 --script http-headers 192.168.1.10**

Анализирует HTTP заголовки ответа сервера.

```
HTTP/1.1 200 OK
Server: nginx/1.24.0
Content-Type: text/html
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000
```

18

$ **nmap -p 443 --script ssl-cert 192.168.1.10**

Получает информацию о TLS сертификате.

```
Subject: CN=example.com
Issued by: CN=Let's Encrypt
Valid from: 2024-01-01
Valid to:   2024-04-01
TLS: TLSv1.3
```

19

$ **nmap -p 443 --script ssl-enum-ciphers 192.168.1.10**

Определяет поддерживаемые TLS протоколы и шифры.

```
TLSv1.2:
- ECDHE-RSA-AES256-GCM-SHA384 (strong)
- ECDHE-RSA-AES128-GCM-SHA256 (strong)
TLSv1.3:
- TLS_AES_256_GCM_SHA384    (strong)
- TLS_AES_128_GCM_SHA256    (strong)
```

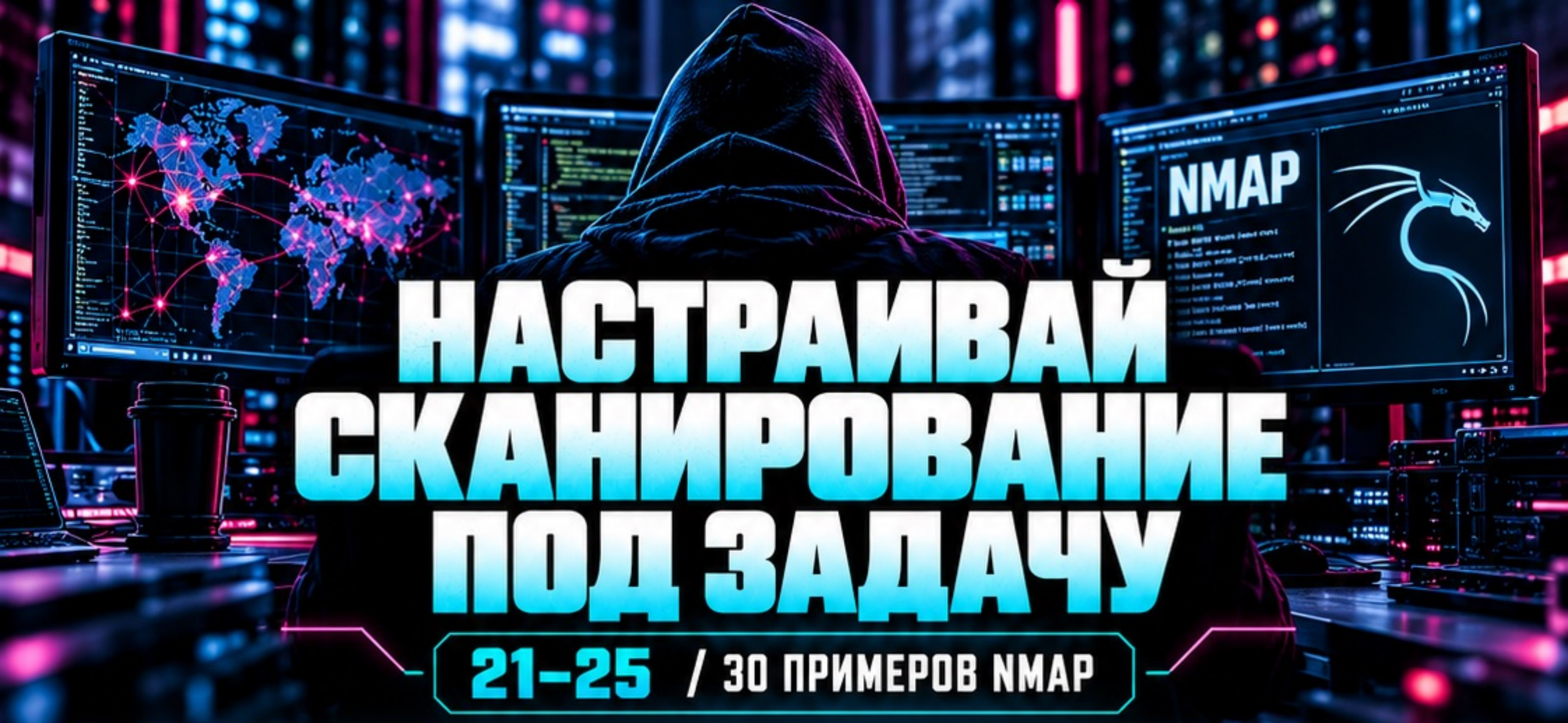
20

$ **nmap -p 22 --script ssh-hostkey 192.168.1.10**

Получает SSH host-key отпечатки, чтобы идентифицировать удалённый хост.

```
22/tcp  open  ssh
| ssh-hostkey:
|   256 SHA256:Ab3... (ECDSA)
|   256 SHA256:Cd8... (ED25519)
|.  2048 SHA256:Ef1... (RSA)
```

Внимательно изучай результаты каждого скрипта. Перебор шифров может занять время и установить много соединений.



НАСТРАИВАЙ СКАНИРОВАНИЕ ПОД ЗАДАЧУ

21–25 / 30 ПРИМЕРОВ NMAP

21

$ **nmap -Pn 192.168.1.10**

Пропускает discovery и считает хост активным (полезно, если ICMP фильтруется).

```
Nmap scan report for 192.168.1.10
Host is up (0.0021s latency).
```

Host is up

22

$ **nmap -n 192.168.1.10**

Отключает reverse DNS resolution для ускорения сканирования.

- Reverse DNS
- Faster scan

23

$ **nmap -T4 192.168.1.10**

Использует более быстрый тайминг для надёжной сети.

T0 – очень медленно
T1 – медленно
T2 – осторожно
T3 – стандартно
T4 – быстро
T5 – очень быстро

24

$ **nmap --max-retries 2 192.168.1.10**

Ограничивает количество повторных попыток, чтобы быстрее получить результат (можно пропустить некоторые ответы).

```
Max retries: 2
1 попытка
2 попытка
3 попытка– ...
```

25

$ **nmap --host-timeout 5m 192.168.1.10**

Прекращает сканирование хоста, если нет ответа в течение 5 минут.

```
Host timeout: 5m
Нет ответа → переход
к следующему хосту
```

Более агрессивные тайминги и жёсткие ограничения могут снизить точность результатов.

СОХРАНЯЙ И АНАЛИЗИРУЙ РЕЗУЛЬТАТЫ

26–30 / 30 ПРИМЕРОВ NMAP

26

$ **nmap -oN scan.txt 192.168.1.10**

Сохраняет результаты сканирования в удобный текстовый файл.

```
# scan.txt
Nmap scan report for 192.168.1.10
Host is up (0.0021s latency).
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
```

27

$ **nmap -oX scan.xml 192.168.1.10**

Сохраняет структурированный вывод в формате XML (удобно для автоматизации).

```
<?xml version="1.0"?>
<nmaprun>
 <host>
  <address addr="192.168.1.10"/>
  <ports>
   <port portid="22" protocol="tcp">
    <state state="open"/>
```

28

$ **nmap -oA scan 192.168.1.10**

Сохраняет сразу несколько форматов: обычный вывод (.nmap), XML (.xml) и формат для grep (.gnmap).

scan.nmap
scan.xml
scan.gnmap

.nmap
.xml
.gnmap

29

$ **nmap --reason 192.168.1.10**

Показывает причины состояний хостов и портов (почему открыт, закрыт или отфильтрован).

```
PORT     STATE    REASON
22/tcp   open     syn-ack
80/tcp   open     syn-ack
443/tcp  filtered no-response
```

30

$ **nmap -v 192.168.1.10**

Подробный вывод во время сканирования (больше деталей о процессе и найденных объектах).

```
Starting Nmap 7.94 ( https://nmap.org )
Scanning 192.168.1.10 [1000 ports]
Discovered open port 22/tcp
Discovered open port 80/tcp
Completed SYN Stealth Scan
Nmap done: 1 host up (0.0021s)
```

Сохраняй результаты каждого сканирования — это упрощает анализ, сравнение изменений и отчётность.