Основы построения защищенных компьютерных сетей

Лекция 4
Сетевой сканер Nmap

Семён Новосёлов

2023

БФУ
ИМЕНИ И. КАНТА

Введение

Nmap — самый популярный и продвинутый сетевой сканер.

Разработчик: Gordon Lyon

nmap.org

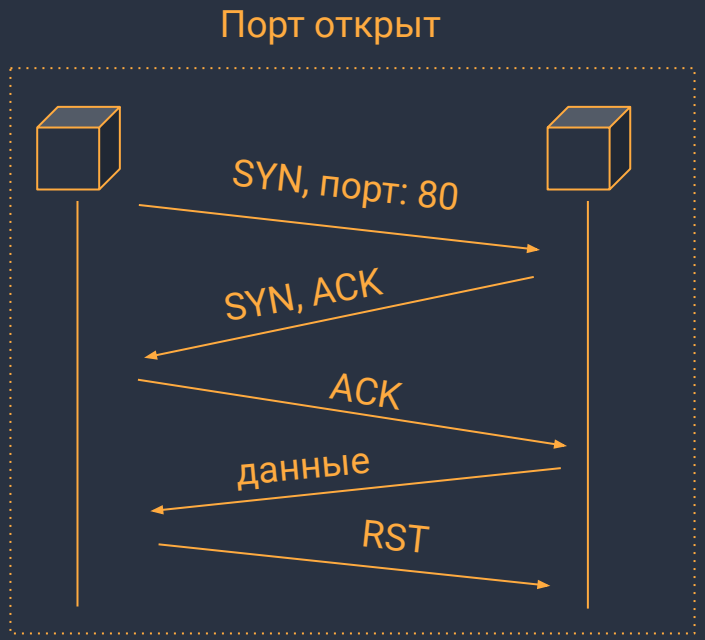
Nmap часто используется в попытках уничтожить мир

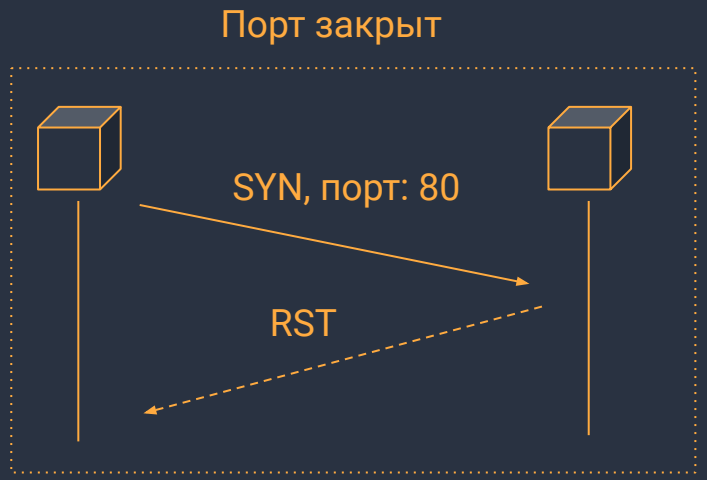
Техники сканирования портов

1. TCP-Connect
2. SYN-сканирования
3. Idle-сканирование

TCP Connect. 1/2

Принцип: попытка подключения по TCP к порту





TCP Connect. 2/2

Преимущества:

- не требует прав администратора, трудно ограничить
- может использоваться с утилитами по типу proxychains

Недостатки:

медленно, передача 5 пакетов

Пример. Сканирование через сеть TOR

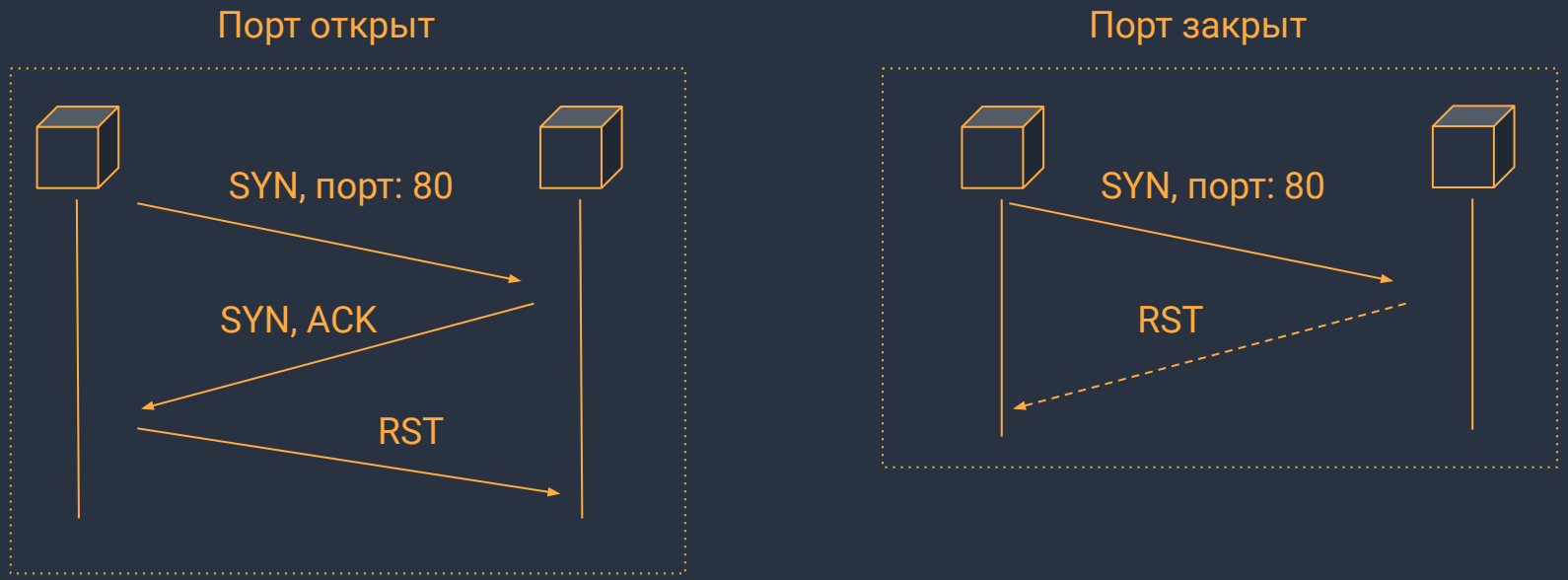

```
proxychains4 nmap -sT -PN -sV --open -n -F ya.ru
```

`proxychains4` перенаправляет все TCP-соединения через цепочку прокси

Важно: протоколы ICMP/UDP/IP не затрагиваются

SYN-сканирование. 1/2

Принцип: закрывать соединение сразу же при получении SYN/ACK



SYN-сканирование. 2/2

Преимущества:

быстрое, передача 3 пакетов

Недостатки:

требует прав администратора,
через proxychains не скрывается

Idle-сканирование. 1/2

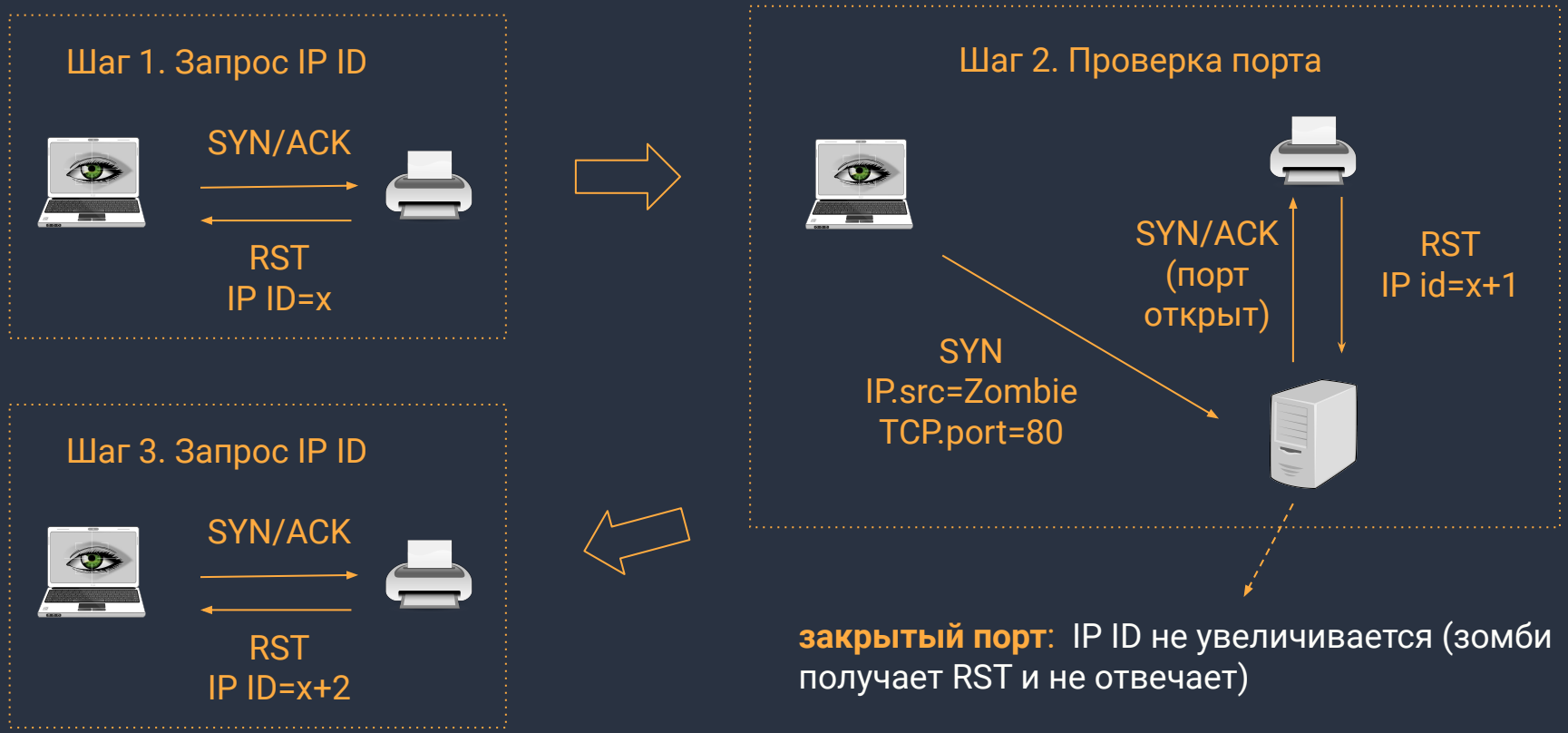
- пакеты не отсылаются на целевую машину напрямую
- скрытое сканирование через зомби-машину
- список открытых портов показывается с точки зрения зомби машины

Зомби

увеличивает IP ID на единицу при получении пакета

Поиск:
nmap --script ipidseq

Idle-сканирование. 2/2



закрытый порт: IP ID не увеличивается (зомби получает RST и не отвечает)

Определение версий сервисов

По баннеру:

текстовым строкам-идентификаторам, посылаемым сервисом

HTTP-заголовки

Server: nginx/1.16.1

Специально составленным запросам:

База **nmap-service-probes**

База запросов Nmap. Пример

```
Probe TCP GetRequest q|GET / HTTP/1.0\r\n\r\n|
ports 1,70,79,80-85, …
sslports 443
```

```
match http m|^HTTP/1\.[01] \d\d\d.*?\r\nServer: nginx\r\n|s p/nginx/ cpe:/a:igor_sysoev:nginx/
```

- `http` — сервис
- `m|^HTTP/1\.[01] \d\d\d.*?\r\nServer: nginx\r\n|s` — regex-шаблон
- `p/nginx/` — информация о версии
- `cpe:/a:igor_sysoev:nginx/` — информация о версии

Nmap Scripting Engine (NSE)

Встроенный скриптовый движок на Lua.

Список скриптов по категориям:

https://nmap.org/nsedoc/lib/nmap.html

Использование:

```
nmap --script http-* 192.168.1.1
nmap --script "not intrusive" 192.168.1.1
```

Пример 1. Перебор паролей

Пустые пароли:

```
nmap --script  mysql-empty-password 192.168.56.101
```

Перебор паролей к ssh/telnet/mysql:

```
nmap --script  ssh-brute 192.168.56.101
nmap --script  telnet-brute 192.168.56.101
nmap --script  mysql-brute 192.168.56.101
```

https://nmap.org/nsedoc/categories/brute.html

Пример 2. Перебор DNS

nmap --script dns-brute yandex.ru

```
C:\>nmap -p 80 --script "dns-brute" yandex.ru
Starting Nmap 7.70 ( https://nmap.org ) at 2022-03-15 14:10 RTZ 1 (ceia)
Nmap scan report for yandex.ru (5.255.255.5)
Host is up (0.0066s latency).
Other addresses for yandex.ru (not scanned): 5.255.255.60 77.88.55.77 77.88.55.80

PORT   STATE SERVICE
80/tcp open  http

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     admin.yandex.ru - 93.158.134.57
|     mx.yandex.ru - 77.88.21.249
|     admin.yandex.ru - 2a02:6b8:0:0:0:0:0:205
|     mx.yandex.ru - 2a02:6b8:0:0:0:0:0:311
|     svn.yandex.ru - 5.255.240.20
|     svn.yandex.ru - 2a02:6b8:0:3400:0:0:2:20
|     mx1.yandex.ru - 77.88.21.249
|     id.yandex.ru - 213.180.204.24
|     id.yandex.ru - 2a02:6b8:0:0:0:0:0:24
|     images.yandex.ru - 2a02:6b8:0:0:0:0:0:242
|     news.yandex.ru - 213.180.193.12
|     news.yandex.ru - 213.180.204.12
|     news.yandex.ru - 87.250.250.12
|     news.yandex.ru - 87.250.251.12
```

связанные с сайтом домены и IP-адреса

при аудите / пентесте имеет смысл их просканировать

Nmap в дикой природе

В **2021** хакер получил доступ к внутренней сети «Российских железных дорог»

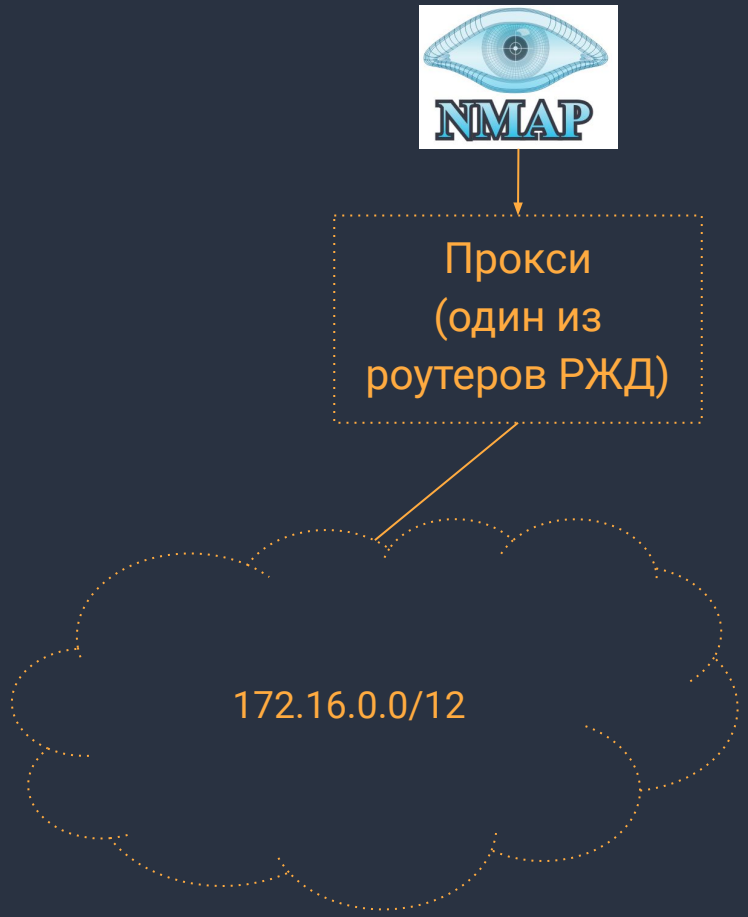
Были доступны:

- около 10 000 камер наблюдения
- IP-телефоны
- система управления кондиционированием и вентиляцией
- и многое другое **...**

Источник и подробности:
https://xakep.ru/2021/01/13/rjd-breach/
https://habr.com/ru/post/536750/

Метод:

- поиск открытых прокси (порт 8080)
- сканирование внутренних сетей (192.168.0.0/16, 172.16.0.0/12) на веб-интерфейсы роутеров/устройств с дефолтным паролем
- получив доступ к роутеру, поднять VPN
- сканировать сеть уже без ограничений по протоколу



Литература и ссылки

- Gordon “Fyodor” Lyon. The Official Nmap Project Guide to Network Discovery and Security Scanning
  https://nmap.org/book/