Nmap - ошибка "Failed to obtain system routes"

Опубликовано muff в Пнд, 2014-10-06 03:11

Понадобилось как-то просканировать хост на открытые порты. Соответственно, инструментом был выбран **Nmap** [1]. Однако не тут-то было.

Запуск сканера вылетал с ошибкой:

```
# nmap muff.kiev.ua

Starting Nmap 6.47 ( http://nmap.org [2] ) at 2014-10-06 02:26 EEST
route_dst_generic: Failed to obtain system routes: getsysroutes_dnet:
sysroutes_dnet_find_interfaces() failed
```

Хм... Утилита не может "подружиться" с сетевым стеком, не находя маршрута к заданому хосту. Более детально вникнув в **man nmap** [3], попытался принудительно указать интерфейс, через который доступен конечный хост:

```
# nmap -e bge0 muff.kiev.ua

Starting Nmap 6.47 ( http://nmap.org [2] ) at 2014-10-06 02:39 EEST
I cannot figure out what source address to use for device bge0, does it even exist?
QUITTING!
```

Да что ж такое... Какие сетевый карты nmap вообще видит?

```
# nmap --iflist

Starting Nmap 6.47 ( http://nmap.org [2] ) at 2014-10-06 02:33 EEST
INTERFACES: NONE FOUND(!)
ROUTES: NONE FOUND(!)
```

Nmap вообще "не видит" сетевых интерфейсов!

После непродолжительного поиска информации в сети, обнаружил, в чем именно проблема. Из ядра я "выпилил" стек **IPv6**, что и привело к тому, что **nmap** "ослеп", хотя в опциях сборки поддержка **IPv6** отключена:

```
# cat /var/db/ports/security_nmap/options

# This file is auto-generated by 'make config'.
# Options for nmap-6.47
_OPTIONS_READ=nmap-6.47
_FILE_COMPLETE_OPTIONS_LIST=DOCS IPV6 SSL
OPTIONS_FILE_SET+=DOCS
```

```
OPTIONS_FILE_UNSET+=IPV6
OPTIONS_FILE_SET+=SSL
```

Однако, не смотря на опции сборки, **nmap** собрался с поддержкой **IPv6**:

```
# nmap --version

Nmap version 6.47 ( http://nmap.org [2] )
Platform: amd64-portbld-freebsd10.0
Compiled with: liblua-5.2.3 openssl-1.0.1e-freebsd libpcre-8.34 libpcap-1.4.0 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: kqueue poll select
```

Нужно что-то с этим делать...

Как вариант - пересобирать ядро с поддержкой **IPv6**.

Либо же запускать **nmap** с ключами "**-sT -Pn**". В этом случае сканер запускается и коректно работает:

```
# nmap -Pn -sT muff.kiev.ua

Starting Nmap 6.47 ( http://nmap.org [2] ) at 2014-10-06 03:06 EEST
Nmap scan report for muff.kiev.ua (91.196.100.50)
Host is up (0.0013s latency).
rDNS record for 91.196.100.50: www.muff.kiev.ua [4]
Not shown: 998 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http


Nmap done: 1 IP address (1 host up) scanned in 41.64 seconds
```

Источник (получено *2025-07-04 00:23*):
http://muff.kiev.ua/content/nmap-oshibka-failed-obtain-system-routes

Ссылки:
[1] http://muff.kiev.ua/content/nmap-skaner-portov
[2] http://nmap.org
[3] http://muff.kiev.ua/content/nmap-network-mapper-utilita-dlya-skanirovaniya-i-issledovaniya-bezopasnosti-seti
[4] http://www.muff.kiev.ua