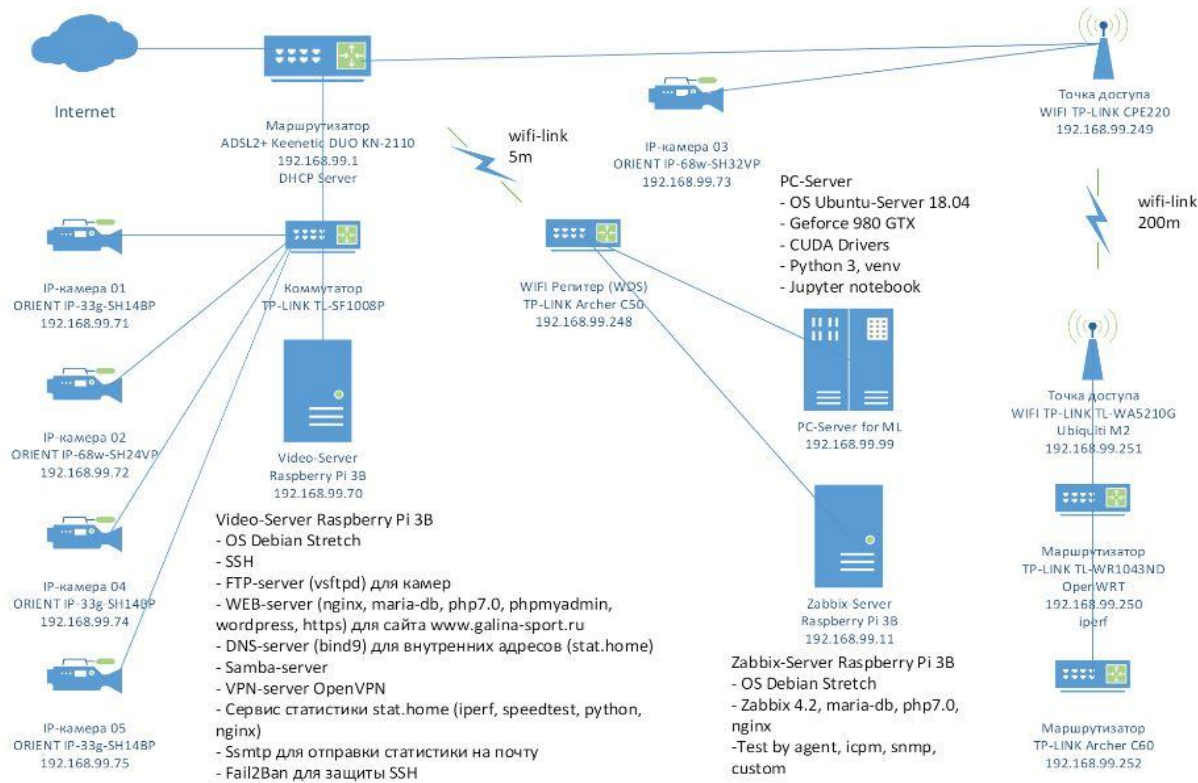


У меня есть небольшая инфраструктура, включая сайт **galina-sport.ru**, который хостится на Raspberry Pi 3. В инфраструктуре много разного железа.



Наружу смотрят порты 80, 443, 20071, 20072, 20073, 20074, 20075, 21194

KEENETIC DUO Поиск настроек

Переадресация ?

Здесь вы можете задать правила переадресации портов, если хотите открыть доступ из Интернета к сервисам вашей сети.

Правила переадресации

Вкл	Вход	Выход	Порты	Описание
<input type="checkbox"/>	PPPoE0	192.168.99.70 RPI3 Debian	tcp/22	22
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.70 RPI3 Debian	tcp/80	80
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.70 RPI3 Debian	tcp/443	443
<input type="checkbox"/>	PPPoE0	192.168.99.70 RPI3 Debian	tcp/1194	1194
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.71 CAMERA_01	tcp/20071	CAMERA_01
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.72 CAMERA_02	tcp/20072	CAMERA_02
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.73 CAMERA_03	tcp/20073	CAMERA_03
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.74 CAMERA_04	tcp/20074	CAMERA_04
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.75 CAMERA_05	tcp/20075	CAMERA_05
<input type="checkbox"/>	PPPoE0	192.168.99.70 RPI3 Debian	udp/21194	VPN udp
<input checked="" type="checkbox"/>	PPPoE0	192.168.99.70 RPI3 Debian	tcp/21194	VPN tcp

[Добавить правило](#) [Удалить все правила](#)

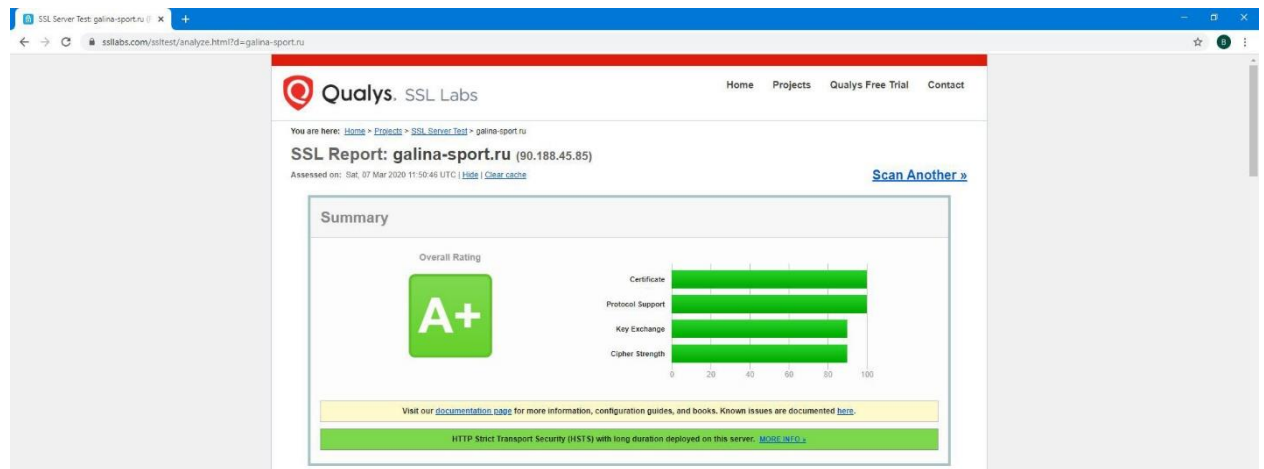
Открытые порты по UPnP

Нет открытых портов

Сайт **galina-sport.ru** малонагруженный, на wordpress, не самые свежие версии nginx, php, давно не обновлял wordpress и плагины к нему.

Но сразу производилась настройка https максимальной защищенности. И скрыл версию nginx в конфигах (и кажется php тоже)

<https://www.ssllabs.com/ssltest/analyze.html?d=galina-sport.ru>



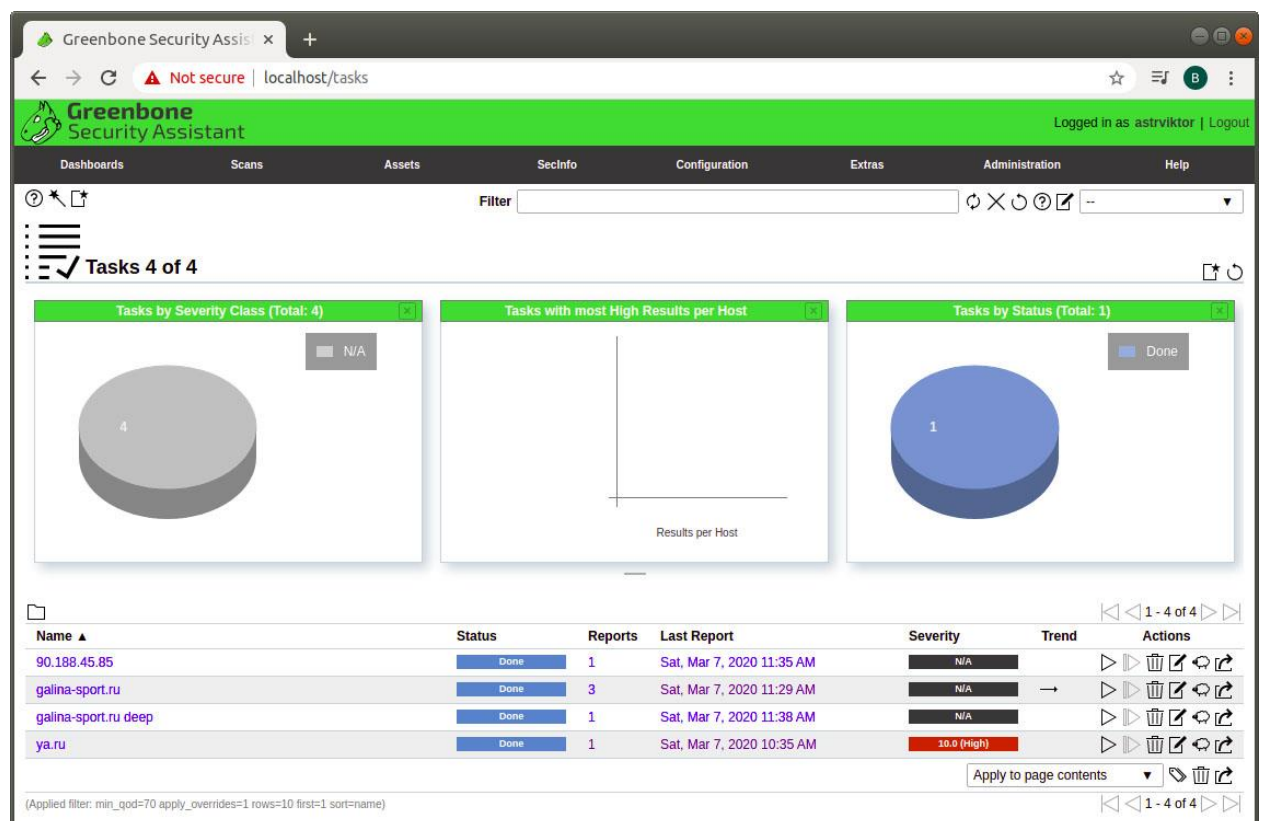
Openvas

С установкой сканера **openvas** пришлось повозиться:

- на Ubuntu 18 из коробки не заработал
- на последней Kali Linux в виртуалке из коробки не заработал
- заработал на Raspberry Pi 3 + Kali Linux, но слишком медленно
- неплохо заработал из под Centos 7

Но сканирование по hostname не дало хороших результатов

Пример сканирования ya.ru и galina-sport.ru

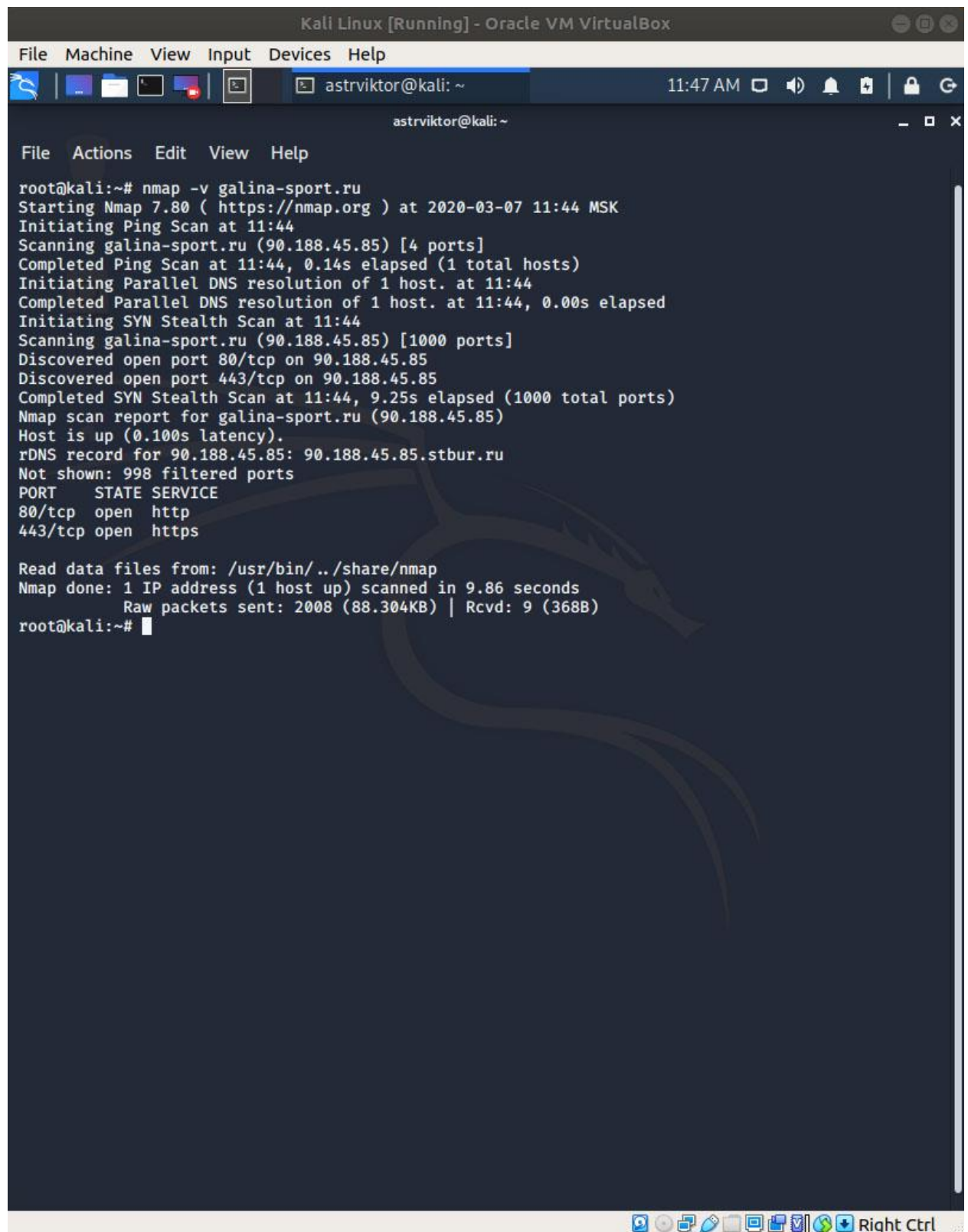


Получается, что у **galina-sport.ru** совсем нет уязвимостей ... что довольно странно :)

Попробуем работу с **Kali Linux** как в статье <https://habr.com/ru/company/pentestit/blog/432014/>

Сканирование по умолчанию

`nmap -v galina-sport.ru`



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
astrvictor@kali: ~ 11:47 AM
astrvictor@kali: ~
File Actions Edit View Help
root@kali:~# nmap -v galina-sport.ru
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 11:44 MSK
Initiating Ping Scan at 11:44
Scanning galina-sport.ru (90.188.45.85) [4 ports]
Completed Ping Scan at 11:44, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:44
Completed Parallel DNS resolution of 1 host. at 11:44, 0.00s elapsed
Initiating SYN Stealth Scan at 11:44
Scanning galina-sport.ru (90.188.45.85) [1000 ports]
Discovered open port 80/tcp on 90.188.45.85
Discovered open port 443/tcp on 90.188.45.85
Completed SYN Stealth Scan at 11:44, 9.25s elapsed (1000 total ports)
Nmap scan report for galina-sport.ru (90.188.45.85)
Host is up (0.100s latency).
rDNS record for 90.188.45.85: 90.188.45.85.stbur.ru
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

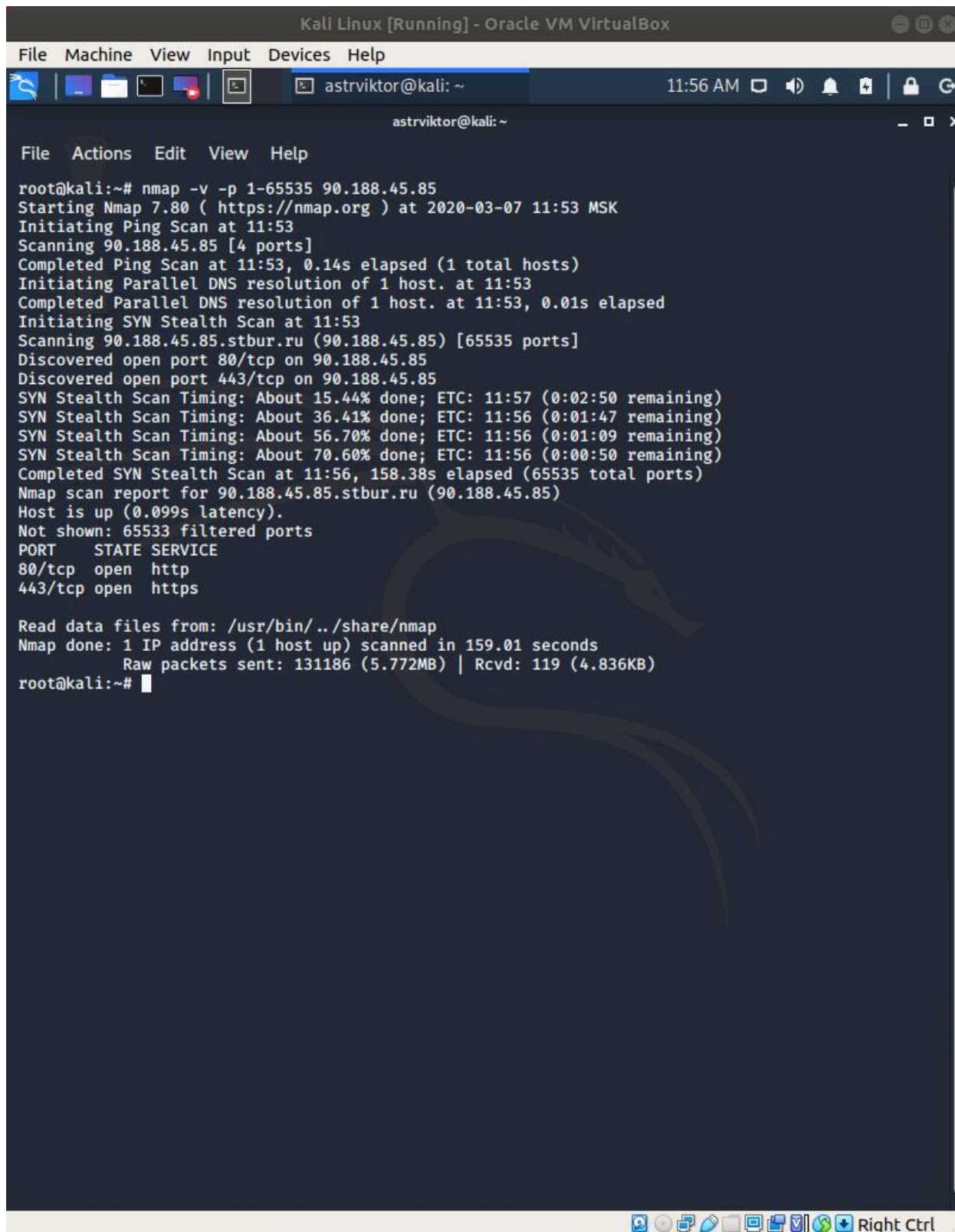
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 9.86 seconds
Raw packets sent: 2008 (88.304KB) | Rcvd: 9 (368B)
root@kali:~#
```

Как и ожидалось, открыты 80 и 443 порты.
Попробуем полное сканирование по портам

Полное сканирование.

```
nmap -v -p 1-65535 90.188.45.85
```

Странно, но нашлись опять только 80 и 443, и больше ничего... пробовал несколько раз ...



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
astrvictor@kali: ~ 11:56 AM
astrvictor@kali: ~
File Actions Edit View Help
root@kali:~# nmap -v -p 1-65535 90.188.45.85
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 11:53 MSK
Initiating Ping Scan at 11:53
Scanning 90.188.45.85 [4 ports]
Completed Ping Scan at 11:53, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:53
Completed Parallel DNS resolution of 1 host. at 11:53, 0.01s elapsed
Initiating SYN Stealth Scan at 11:53
Scanning 90.188.45.85.stbur.ru (90.188.45.85) [65535 ports]
Discovered open port 80/tcp on 90.188.45.85
Discovered open port 443/tcp on 90.188.45.85
SYN Stealth Scan Timing: About 15.44% done; ETC: 11:57 (0:02:50 remaining)
SYN Stealth Scan Timing: About 36.41% done; ETC: 11:56 (0:01:47 remaining)
SYN Stealth Scan Timing: About 56.70% done; ETC: 11:56 (0:01:09 remaining)
SYN Stealth Scan Timing: About 70.60% done; ETC: 11:56 (0:00:50 remaining)
Completed SYN Stealth Scan at 11:56, 158.38s elapsed (65535 total ports)
Nmap scan report for 90.188.45.85.stbur.ru (90.188.45.85)
Host is up (0.099s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 159.01 seconds
Raw packets sent: 131186 (5.772MB) | Rcvd: 119 (4.836KB)
root@kali:~#
```

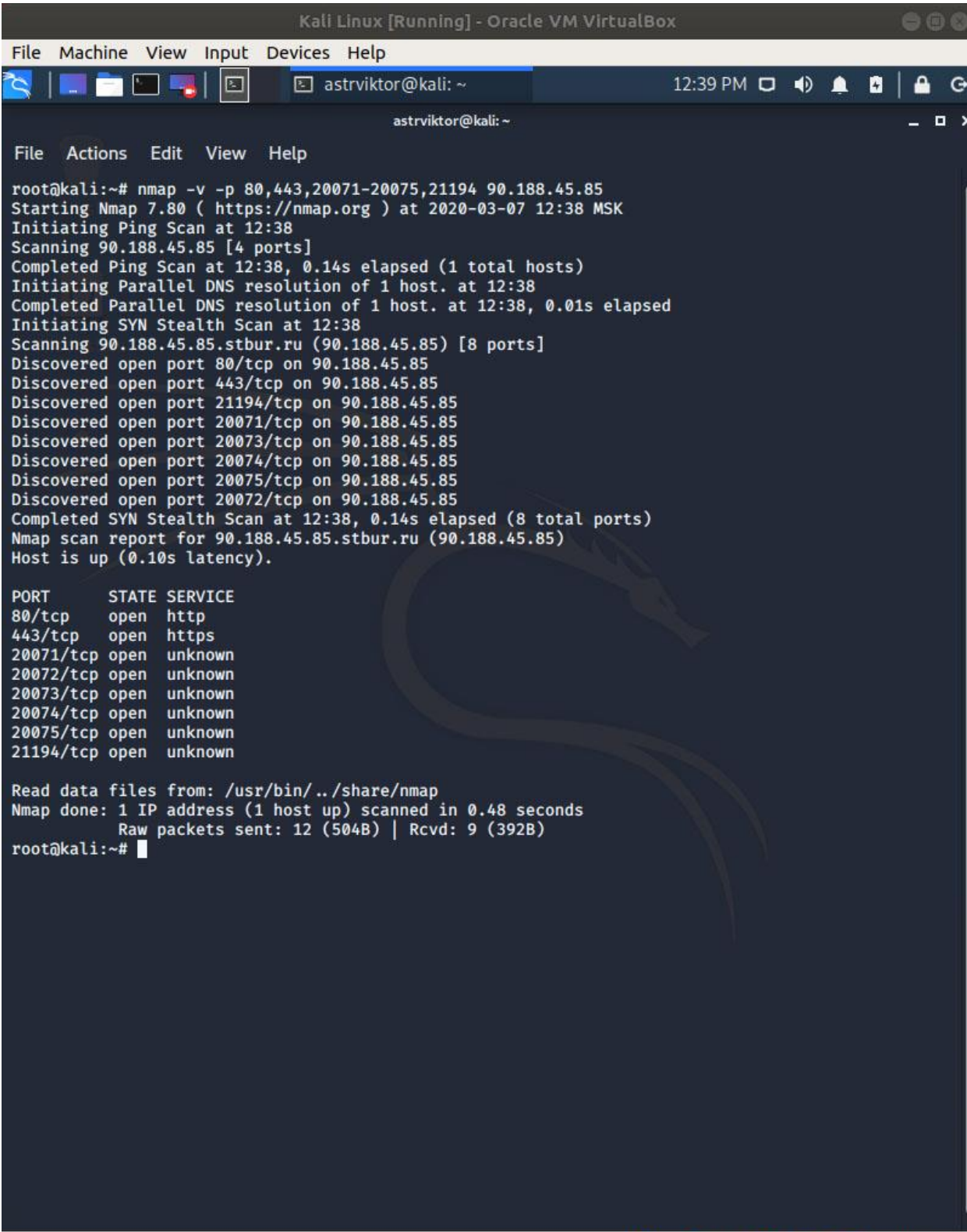
Но мы уже знаем, что открытые порты 80, 443, 20071, 20072, 20073, 20074, 20075, 21194

Попробуем проверить конкретные порты

Проверим, видит ли их nmap целенаправленно. Оказалось, что сканирование по всему диапазону не всегда работает, но целенаправленно nmap порты видит

Сканируем конкретные порты

```
nmap -v -p 80,443,20071-20075,21194 90.188.45.85
```



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
astrvictor@kali: ~
12:39 PM
astrvictor@kali: ~
File Actions Edit View Help
root@kali:~# nmap -v -p 80,443,20071-20075,21194 90.188.45.85
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 12:38 MSK
Initiating Ping Scan at 12:38
Scanning 90.188.45.85 [4 ports]
Completed Ping Scan at 12:38, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:38
Completed Parallel DNS resolution of 1 host. at 12:38, 0.01s elapsed
Initiating SYN Stealth Scan at 12:38
Scanning 90.188.45.85.stbur.ru (90.188.45.85) [8 ports]
Discovered open port 80/tcp on 90.188.45.85
Discovered open port 443/tcp on 90.188.45.85
Discovered open port 21194/tcp on 90.188.45.85
Discovered open port 20071/tcp on 90.188.45.85
Discovered open port 20073/tcp on 90.188.45.85
Discovered open port 20074/tcp on 90.188.45.85
Discovered open port 20075/tcp on 90.188.45.85
Discovered open port 20072/tcp on 90.188.45.85
Completed SYN Stealth Scan at 12:38, 0.14s elapsed (8 total ports)
Nmap scan report for 90.188.45.85.stbur.ru (90.188.45.85)
Host is up (0.10s latency).

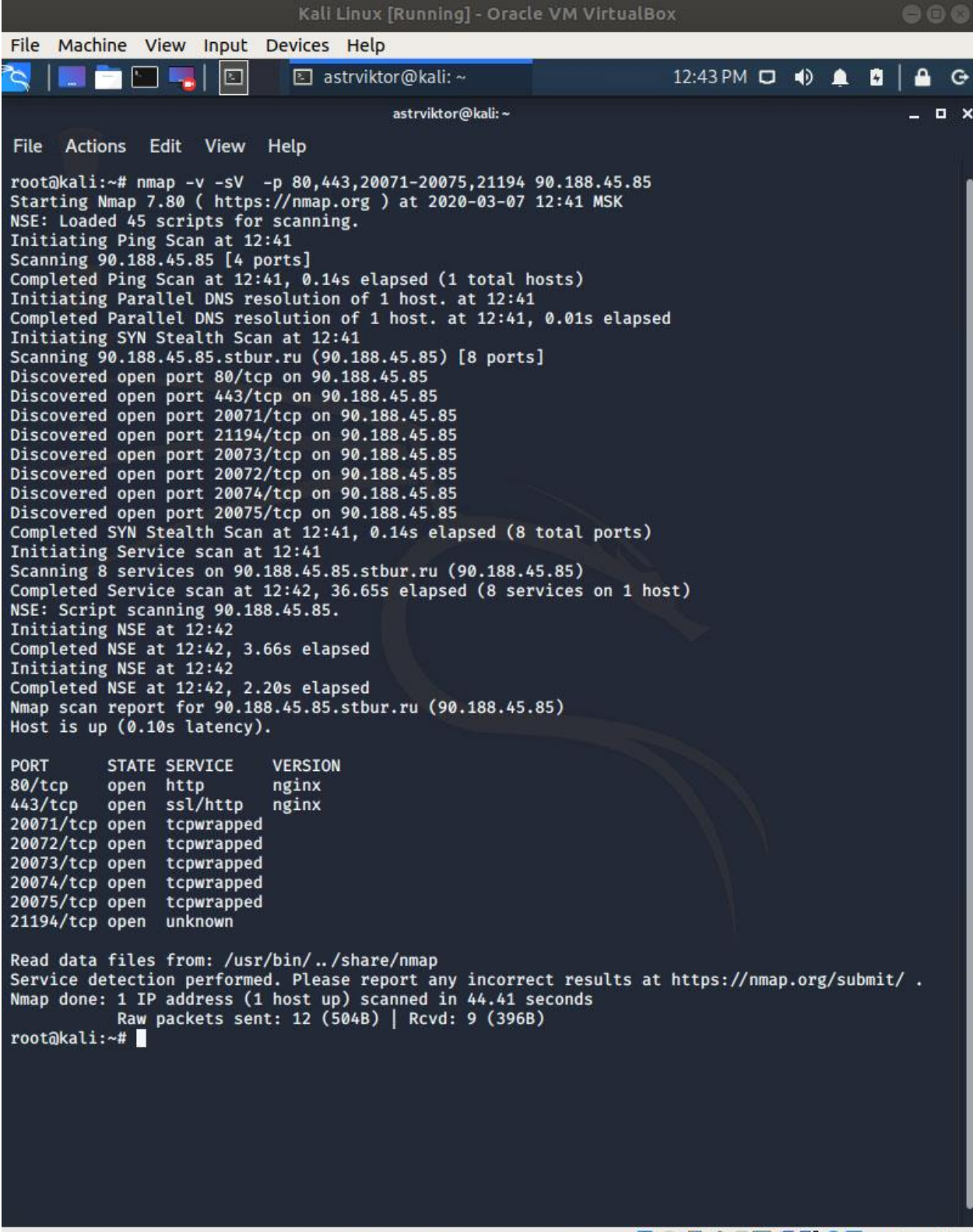
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
20071/tcp open  unknown
20072/tcp open  unknown
20073/tcp open  unknown
20074/tcp open  unknown
20075/tcp open  unknown
21194/tcp open  unknown

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
Raw packets sent: 12 (504B) | Rcvd: 9 (392B)
root@kali:~#
```

Да, все порты про которые мы знаем, открыты

Пробуем определить, что там за сервисы на этих портах

```
nmap -v -sV -p 80,443,20071-20075,21194 90.188.45.85
```



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
astrvictor@kali: ~ 12:43 PM
astrvictor@kali: ~
File Actions Edit View Help
root@kali:~# nmap -v -sV -p 80,443,20071-20075,21194 90.188.45.85
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 12:41 MSK
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 12:41
Scanning 90.188.45.85 [4 ports]
Completed Ping Scan at 12:41, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:41
Completed Parallel DNS resolution of 1 host. at 12:41, 0.01s elapsed
Initiating SYN Stealth Scan at 12:41
Scanning 90.188.45.85.stbur.ru (90.188.45.85) [8 ports]
Discovered open port 80/tcp on 90.188.45.85
Discovered open port 443/tcp on 90.188.45.85
Discovered open port 20071/tcp on 90.188.45.85
Discovered open port 21194/tcp on 90.188.45.85
Discovered open port 20073/tcp on 90.188.45.85
Discovered open port 20072/tcp on 90.188.45.85
Discovered open port 20074/tcp on 90.188.45.85
Discovered open port 20075/tcp on 90.188.45.85
Completed SYN Stealth Scan at 12:41, 0.14s elapsed (8 total ports)
Initiating Service scan at 12:41
Scanning 8 services on 90.188.45.85.stbur.ru (90.188.45.85)
Completed Service scan at 12:42, 36.65s elapsed (8 services on 1 host)
NSE: Script scanning 90.188.45.85.
Initiating NSE at 12:42
Completed NSE at 12:42, 3.66s elapsed
Initiating NSE at 12:42
Completed NSE at 12:42, 2.20s elapsed
Nmap scan report for 90.188.45.85.stbur.ru (90.188.45.85)
Host is up (0.10s latency).

PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx
443/tcp   open  ssl/http     nginx
20071/tcp open  tcpwrapped
20072/tcp open  tcpwrapped
20073/tcp open  tcpwrapped
20074/tcp open  tcpwrapped
20075/tcp open  tcpwrapped
21194/tcp open  unknown

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.41 seconds
Raw packets sent: 12 (504B) | Rcvd: 9 (396B)
root@kali:~#
```

Как и ожидалось:

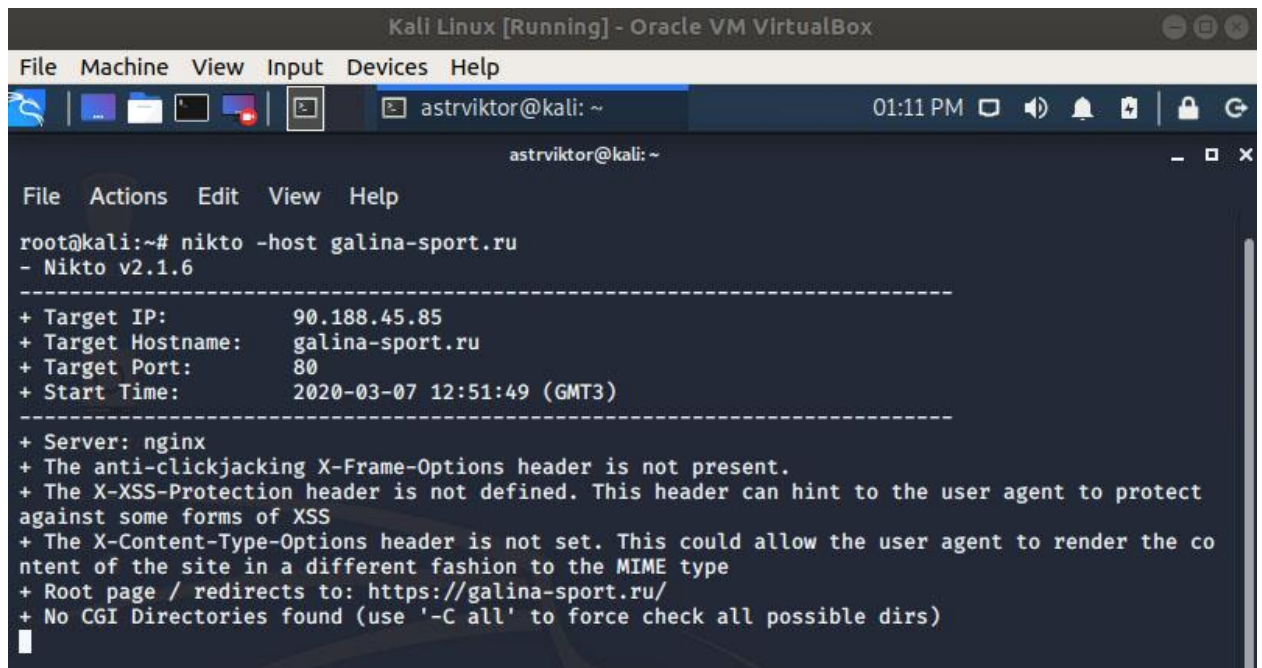
- 80,443 – nginx (без конкретной версии, что плюс)
- 20071-20075 - tcpwrapped (тут rtsp трафик)
- 21194 - unknown (на самом деле openvpn)

Попробуем определить, что там стоит за nginx

Используя инструмент nikto, мы должны определить, что вероятнее всего используется CMS WordPress.

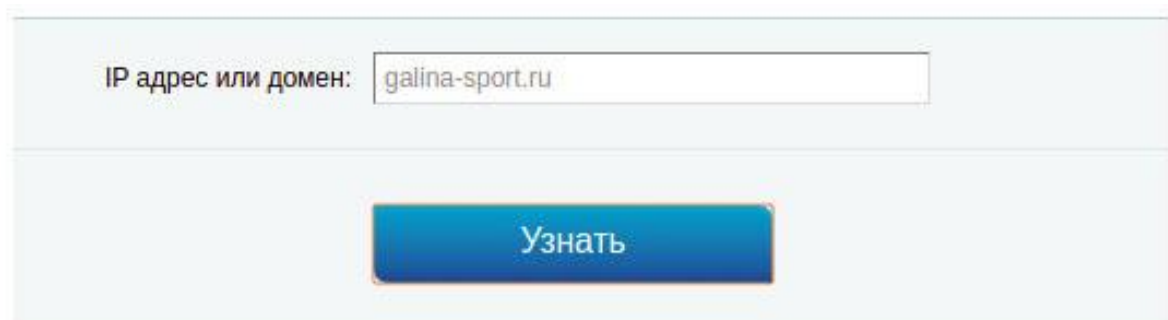
nikto -host galina-sport.ru:80

Работала очень долго...была остановлена



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
astrvictor@kali: ~
01:11 PM
astrvictor@kali: ~
File Actions Edit View Help
root@kali:~# nikto -host galina-sport.ru
- Nikto v2.1.6
-----
+ Target IP: 90.188.45.85
+ Target Hostname: galina-sport.ru
+ Target Port: 80
+ Start Time: 2020-03-07 12:51:49 (GMT3)
-----
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://galina-sport.ru/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

На самом деле более быстрый способ получить CMS сайта - <https://2ip.ru/cms/>
Отработало за пару минут



IP адрес или домен:

[Узнать](#)

CMS	Результат
1С:Битрикс	признаков использования не найдено
WordPress	найлены признаки использования
Drupal	признаков использования не найдено
Joomla!	признаков использования не найдено
NetCat	признаков использования не найдено
UMI.CMS	признаков использования не найдено
MODx	признаков использования не найдено

Итак, у нас wordpress причем не самый новый (мы это знаем) и там установлены какие то плагины (которые тоже давно не обновлялись), возможно тут есть уязвимости...

Просканируем WPScan сразу с ключем --plugins-detection aggressive

wpscan --url galina-sport.ru --plugins-detection aggressive

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
astrviktor@kali: ~
01:52 PM
astrviktor@kali: ~
File Actions Edit View Help
root@kali:~# wpscan --url galina-sport.ru --plugins-detection aggressive

-----
  WPScan
WordPress Security Scanner by the WPScan Team
Version 3.7.8
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
-----

[+] URL: http://galina-sport.ru/
[+] Effective URL: https://galina-sport.ru/
[+] Started: Sat Mar 7 13:15:49 2020

Interesting Finding(s):

[+] https://galina-sport.ru/
  Interesting Entries:
  - server: nginx
  - content-security-policy: block-all-mixed-content
  Found By: Headers (Passive Detection)
  Confidence: 100%

[+] https://galina-sport.ru/xmlrpc.php
  Found By: Link Tag (Passive Detection)
  Confidence: 100%
  Confirmed By: Direct Access (Aggressive Detection), 100% confidence
  References:
  - http://codex.wordpress.org/XML-RPC_Pingback_API
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress version 4.9.10 identified (Insecure, released on 2019-03-13).
  Found By: Rss Generator (Passive Detection)
  - https://galina-sport.ru/feed/, <generator>https://wordpress.org/?v=4.9.10</generator>
  - https://galina-sport.ru/comments/feed/, <generator>https://wordpress.org/?v=4.9.10</generator>

[+] WordPress theme in use: dream
  Location: http://galina-sport.ru/wp-content/themes/dream/
  Latest Version: 1.0.21 (up to date)
  Last Updated: 2018-03-24T00:00:00.000Z
  Style URL: https://galina-sport.ru/wp-content/themes/dream/style.css?ver=1.0.22
  Style Name: Dream
  Style URI: http://vsfish.com/themes/dream/
  Description: Dream is fully responsive WordPress theme....
  Author: vsFish
  Author URI: http://vsfish.com/

  Found By: Css Style In Homepage (Passive Detection)

  Version: 1.0.24 (80% confidence)
  Found By: Style (Passive Detection)
  - https://galina-sport.ru/wp-content/themes/dream/style.css?ver=1.0.22, Match: 'Version: 1.0.24'

[+] Enumerating All Plugins (via Aggressive Methods)
[+] Checking Known Locations - Time: 00:35:38 <===== > (39964 / 85245) 46.88% ETA: 00:40:23
```


Сканировалось на уязвимости (85245 известных плагинов) больше часа, и нашло: ничего полезного не нашлось...

```
[+] Enumerating All Plugins (via Aggressive Methods)
Checking Known Locations - Time: 01:14:52 <=====> (85245 / 85245) 100.00% Time: 01:14:52

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:01 <=====> (21 / 21) 100.00% Time: 00:00:01

[i] No Config Backups Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvuln.db.com/users/sign_up

[+] Finished: Sat Mar 7 14:32:03 2020
[+] Requests Done: 85268
[+] Cached Requests: 38
[+] Data Sent: 39.499 MB
[+] Data Received: 18.465 MB
[+] Memory used: 381.566 MB
[+] Elapsed time: 01:16:14
root@kali:~#
```

Raspberry Pi 3

На текущем момент конфигурация web сервисов следующая:

nginx -v

nginx version: nginx/1.10.3

php -v

PHP 7.0.33-0+deb9u3 (cli) (built: Mar 8 2019 10:01:24) (NTS)

Copyright (c) 1997-2017 The PHP Group

Zend Engine v3.0.0, Copyright (c) 1998-2017 Zend Technologies

with Zend OPcache v7.0.33-0+deb9u3, Copyright (c) 1999-2017, by Zend Technologies

Рекомендации

Обновляйте всегда, особенно уязвимости безопасности, но лучше через несколько дней после выхода новых версий (вдруг в новых версиях проблемы)

Обновляйте систему

Обновляйте прошивки железа

Обновляйте nginx

Обновляйте php

Обновляйте wordpress

Обновляйте плагины

Важно: на текущий момент в облаке без ssh скорее всего никак не обойтись.

Используйте fail2ban для ssh и подобные инструменты.

Ссылка на мою настройку (с fail2ban) vpn сервера на DigitalOcean:

<https://github.com/astrviktor/linux/blob/master/do-vpn.txt>