```
25/tcp   open  smtp          Postfix smtpd
|_smtp-commands: [redacted], PIPELINING, SIZE 20000000, STARTTLS, AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
SMTPUTF8,
| ssl-cert: Subject: commonName=[redacted]
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2020-04-30T22:32:52+00:00
| Not valid after:  2020-07-29T22:32:52+00:00
| MD5:   400d cad6 5442 f2b5 0d93 4705 8e7e d33f
|_SHA-1: ec33 8715 e903 2805 265e 171e c27c 3c55 5a5d 90cb
|_ssl-date: 2004-09-28T23:49:43+00:00; -15y257d15h28m24s from local time.
80/tcp   open  http          nginx
|_http-methods: No Allow or Public header in OPTIONS response (status code 405)
|_http-title: Welcome to nginx!
143/tcp  open  imap          Dovecot imapd
|_imap-capabilities: IMAP4rev1 listed Pre-login ID OK post-login AUTH=PLAIN AUTH=LOGINA0001 SASL-IR IDLE more STARTTLS have LITERAL+ LOGIN-REFERRALS ENABLE
capabilities
```


Небольшой практический совет. Время от времени рекомендую сканировать свои внешние ip адреса какими-нибудь сканерами портов, например, nmap. Можно это делать на регулярной основе с помощью скриптов и отправлять отчет себе на почту. Если не делать таких проверок, то рано или поздно что-то забудете заблокировать.

Пример, как это бывает обычно у меня. Поднимается временно какой-то сервис для теста в отдельной виртуальной машине. Для простоты к нему просто

пробрасывается определенный порт. После теста виртуальная машина удаляется, а проброс порта остается. Через некоторое время на этот же ip адрес может приехать что-то другое. Например, у меня приехал новый сервер и на этот ip был посажен idrac. Каково же было мое удивление, когда я, сканируя внешний ip, увидел доступ к консоли управления сервером. Сначала перепугался, думал кто-то что-то сломал. Полез разбираться, оказалось, что старый проброс 443 порта остался на этом внешнем ip.

Вот еще один пример. Стоял тестовый гипервизор HyperV, подключенный в том числе к WAN порту. Подключили на всякий случай, вдруг пригодится. В момент установки и настройки внешний ip ему никто не настраивал, так как он был не нужен. Может интерфейс отключили или что-то еще сделали. Не суть важно. В какой-то момент конфигурировали виртуальные свитчи, в том числе на этом интерфейсе. Он стал активен и автоматом получил настройки внешнего ip по dhcp. Заметил случайно. Сколько HyperV провисел всеми своими портами, в том числе и rdp в интернете — не известно.

Самый простой пример, как можно автоматизировать сканирование внешних ip адресов. Поставьте nmap на какой-то внешний по отношению к тестируемым серверам сервер. И с него по крону раз в неделю запускайте проверку с отправкой результата вам на почту:

```
nmap -T4 -A -v 111.222.333.444 | mail -s "Nmap Scan 111.222.333.444" zeroxzed@gmail.com
```

Если почта через консоль не отправляется, почитайте у меня, как это исправить — отправка почты через консоль linux.

Получите подробный отчет по всем типовым портам, которые открыты на вашем ip адресе.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2020-06-12 18:17 MSK
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 18:17
Scanning [redacted]
Completed Ping Scan at 18:17, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:17
Completed Parallel DNS resolution of 1 host. at 18:17, 0.03s elapsed
Initiating SYN Stealth Scan at 18:17
Scanning [redacted] [1000 ports]
Discovered open port 443/tcp on [redacted]
Discovered open port 25/tcp on [redacted]
Discovered open port 80/tcp on [redacted]
Discovered open port 993/tcp on [redacted]
Discovered open port 143/tcp on [redacted]
Discovered open port 587/tcp on [redacted]
Discovered open port 1199/tcp on [redacted]
Discovered open port 1198/tcp on [redacted]
Discovered open port 5222/tcp on [redacted]
Discovered open port 9998/tcp on [redacted]
Completed SYN Stealth Scan at 18:17, 15.19s elapsed (1000 total ports)
Initiating Service scan at 18:17
Scanning 10 services on [redacted]
Completed Service scan at 18:18, 26.11s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against [redacted]
Retrying OS detection (try #2) against [redacted]
Initiating Traceroute at 18:18
```

Ниже в отчете будет информация о работающих сервисах. Имеет смысл просматривать и их.

```
25/tcp   open  smtp          Postfix smtpd
|_smtp-commands: [redacted], PIPELINING, SIZE 20000000, STARTTLS, AUTH PLAIN LOGIN, AUTH=PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
SMTPUTF8,
| ssl-cert: Subject: commonName=[redacted]
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2020-04-30T22:32:52+00:00
| Not valid after:  2020-07-29T22:32:52+00:00
| MD5:   400d cad6 5442 f2b5 0d93 4705 8e7e d33f
|_SHA-1: ec33 8715 e903 2805 265e 171e c27c 3c55 5a5d 90cb
|_ssl-date: 2004-09-28T23:49:43+00:00; -15y257d15h28m24s from local time.
80/tcp   open  http          nginx
|_http-methods: No Allow or Public header in OPTIONS response (status code 405)
|_http-title: Welcome to nginx!
143/tcp  open  imap          Dovecot imapd
|_imap-capabilities: IMAP4rev1 listed Pre-login ID OK post-login AUTH=PLAIN AUTH=LOGINA0001 SASL-IR IDLE more STARTTLS have LITERAL+ LOGIN-REFERRALS ENABLE
capabilities
```


Если у вас небольшая инфраструктура, достаточно раз в неделю просматривать отчеты, чтобы убедиться, что все в порядке. Иначе надо как-то автоматизировать эти проверки. В принципе, ничего сложного нет. Можно с помощью того же Zabbix следить за разрешенным списком открытых портов. Но я не прорабатывал этот вопрос, так как нет надобности. Думаю, что по этой теме уже есть готовые наработки.

программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте . Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области. Особенности курсов:

- Знания, ориентированные на практику;
- Реальные ситуации и задачи;
- Лучшее из международных программ.