Молдавский Государственный Университет Факультет Математики и Информатики Департамент Информатики

Работа по дисциплине

“ SMAI”

Тема работы N2: “ Основы сетей.”

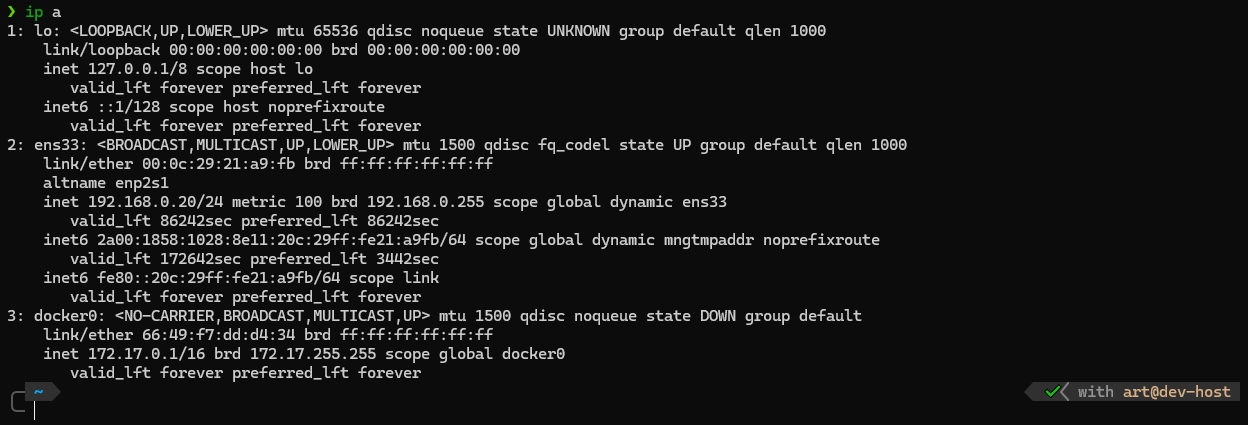
Выполнил: студент группы I2302 Мамалига Артур

Преподаватель: Dumitru Borș

Кишинев 2025

# Часть 1: Базовая диагностика

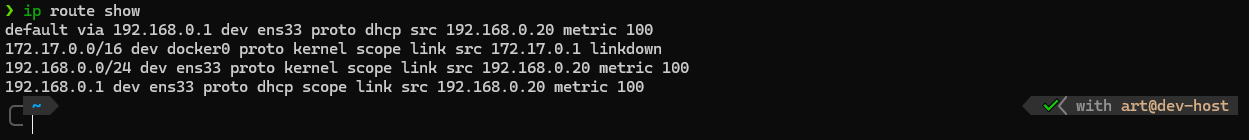
Была проведена проверка сетевых интерфейсов.



Команда ip a показала наличие трёх интерфейсов:

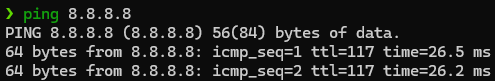
* lo(Loopback) – unix сокеты, для локальных соединений внутри системы, не требует tcp посдключения.
* ens33 – виртуальный физический интерфейс виртуальной машины, через который обеспечивается основной сетевой доступ(проброшен через bridge на хостовую систему).
* Docker0 – Виртуальный интерфейс для докер контейнеров.

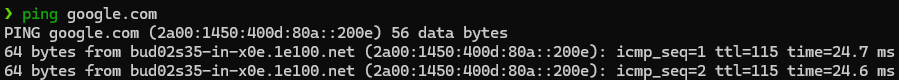
Далее был рассмотрен список статических маршрутов с помощью команды ip route show.



* Маршрут по умолчанию (default) указывает на шлюз 192.168.0.2 через интерфейс ens33;
* Локальная сеть 192.168.0.0/24 также доступна через интерфейс ens33;
* Сеть Docker (172.17.0.0/16) привязана к виртуальному интерфейсу docker0.

Проверка сетевого подключения с помощью команды ping.

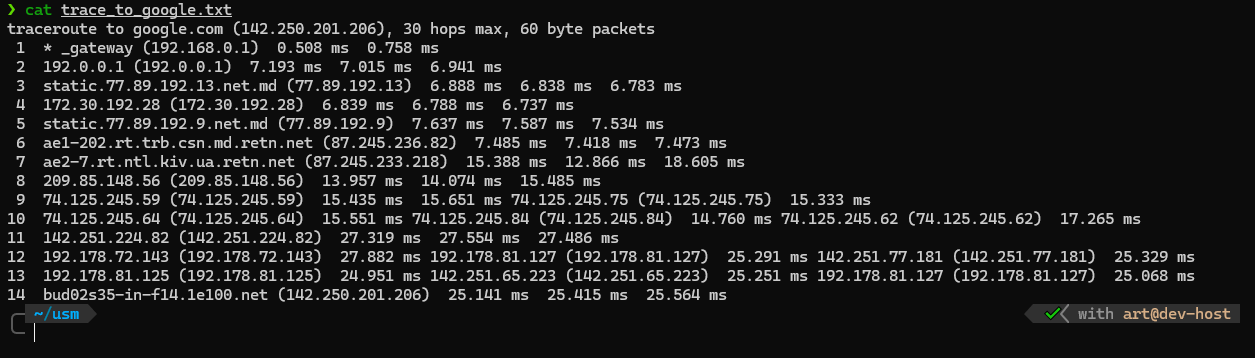




Если DNS работает - ping google.com успешно резолвит имя в IP, пакеты идут.

Если DNS сломан - ping 8.8.8.8 будет работать (доступ по IP), но ping google.com не сможет найти адрес (ошибка unknown host).

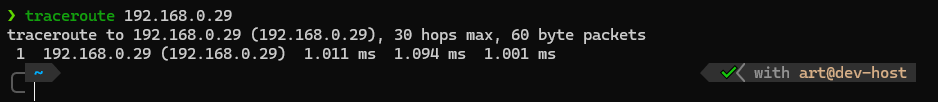
# Часть 2: Маршруты и трассировка



* 192.168.0.1 — твой локальный шлюз (роутер).
* 192.0.0.1 — следующий hop у провайдера.
* 77.89.192.13 — сетка net.md.
* 172.30.192.28 — внутренняя сеть провайдера orange.
* 77.89.192.9 — провайдер.
* 87.245.236.82 — транзит.
* 87.245.233.218 — узел транзитного провайдера видимо.
* 209.85.148.56 — Google.
* 9–14. Несколько узлов Google (74.125.\*, 142.251.\*) → конечный сервер: 142.250.201.206 (google.com).

Маршрут включает локальную сеть, внутренние узлы, транзитные магистрали и глобальную инфраструктуру Google.

Для проверки локального подключения выполнен traceroute до IP-адреса 192.168.0.29.



Подключение осуществляется через Linksys router, работающий в режиме bridge, поэтому хосты взаимодействуют напрямую без дополнительных промежуточных маршрутизаторов.

# Часть 3: порты и соединения

Для анализа открытых портов использовалась команда netstat -tulpen. Результат показал, что на системе прослушиваются только два порта:

* 53/tcp — служба DNS (systemd-resolved).
* 22/tcp — служба SSH.

Таким образом, система минимально открыта во внешнюю сеть, что повышает её безопасность.



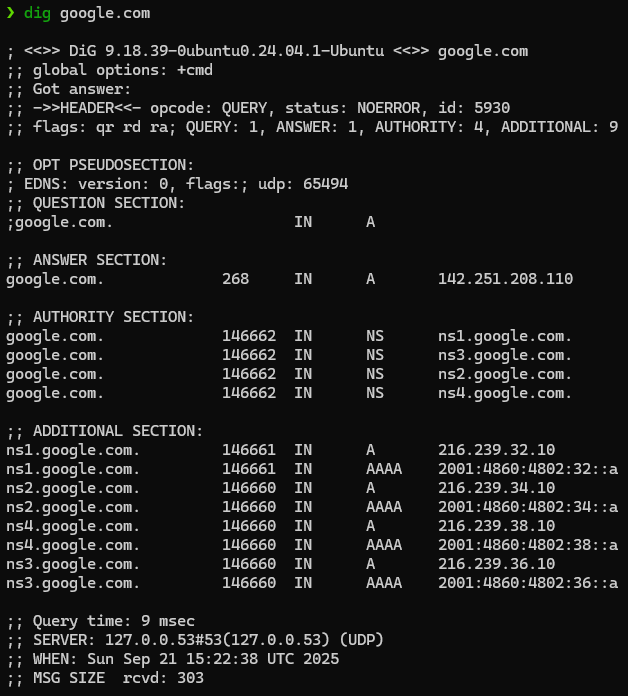
Для демонстрации работы портов использовалась утилита nc (netcat). На хосте был открыт порт 12345, и при подключении клиента успешно прошла передача тестового сообщения hello. Это подтверждает корректное функционирование механизма TCP-соединений на уровне приложений(7).



# Часть 4: Работа с DNS

Для анализа работы системы доменных имён использовались утилиты dig и resolvectl.

Проверка A-записей (dig google.com)

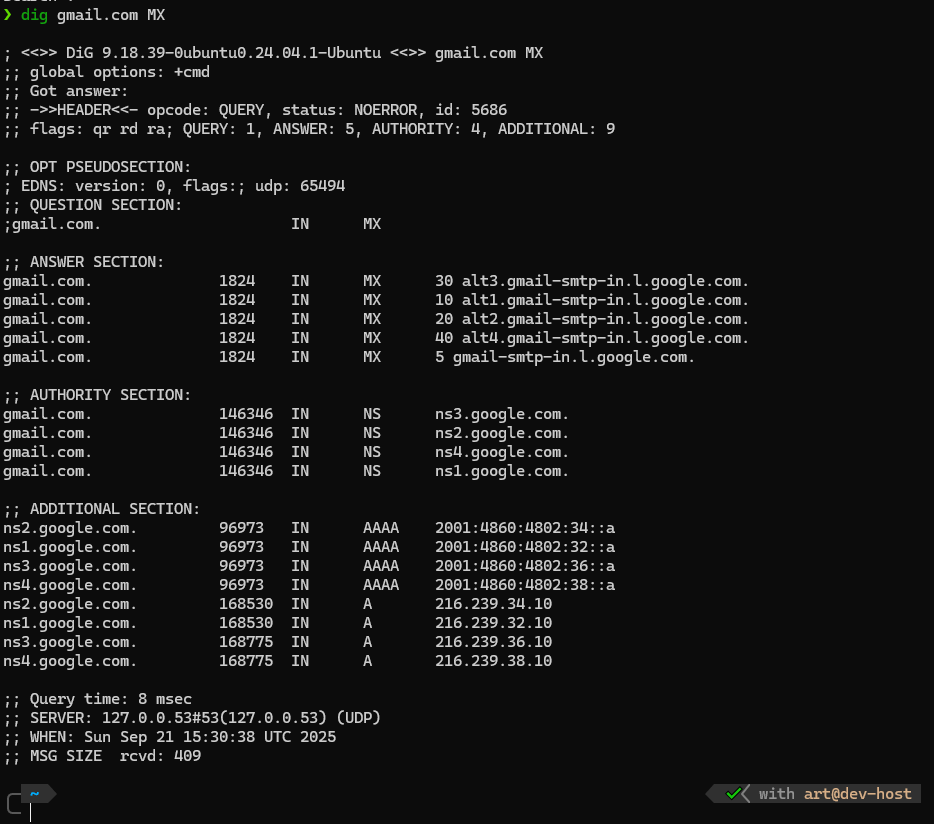


Запрос вернул следующие результаты:

* В секции **ANSWER** доменное имя google.com успешно разрешено в IPv4-адрес: 142.251.208.110.
* В секции **AUTHORITY** указаны авторитетные серверы Google (ns1.google.com, ns2.google.com, ns3.google.com, ns4.google.com).
* В секции **ADDITIONAL** предоставлены дополнительные адреса NS-серверов, как в формате IPv4, так и IPv6.

Таким образом, DNS разрешение работает корректно: имя google.com резолвится в IP-адрес, а также возвращаются данные об инфраструктуре DNS Google.

Проверка MX-записей

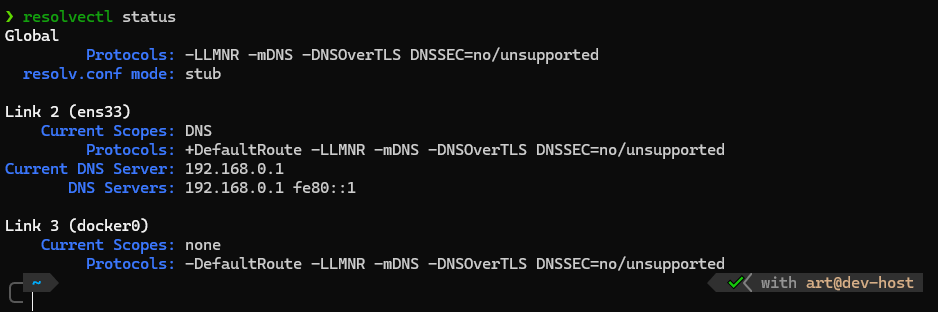


Запрос dig gmail.com MX выдал список почтовых серверов Google:

* alt3.gmail-smtp-in.l.google.com (приоритет 30)
* alt1.gmail-smtp-in.l.google.com (приоритет 10)
* alt2.gmail-smtp-in.l.google.com (приоритет 20)
* alt4.gmail-smtp-in.l.google.com (приоритет 40)
* gmail-smtp-in.l.google.com (приоритет 5)

MX-записи указывают на SMTP-сервера, принимающие почту для домена gmail.com. Более низкое значение приоритета означает более высокий приоритет при доставке сообщений.

DNS-серверы системы:



С помощью команды resolvectl status была получена информация о DNS-настройках:

* Для интерфейса ens33 в качестве DNS-сервера используется шлюз 192.168.0.1.
* Дополнительно настроен адрес fe80::1 для IPv6.
* Для интерфейса docker0 DNS-сервер не задан.

# Часть 5: Сетевой отчет по сайту usm.md

## 1. DNS-записи

С помощью утилиты dig были получены следующие записи:

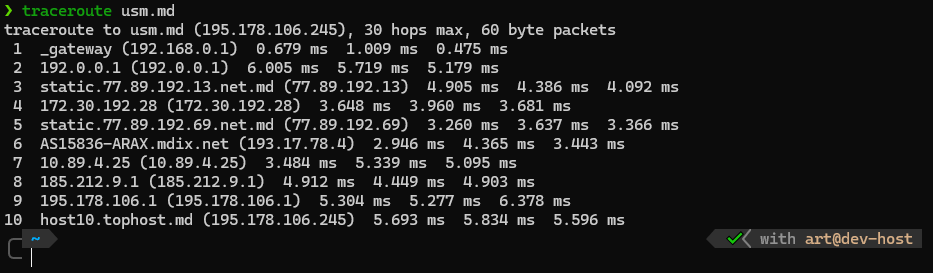
* A-запись:  
  usm.md. - 195.178.106.245 - основной IPv4-адрес сайта.
* MX-записи:  
  usm.md. - usm-md.mail.eo.outlook.com (приоритет 1) - домен обслуживается через сервисы Microsoft Outlook.
* NS-записи:  
  usm.md. - ns.renam.md, ns.usm.md - ответственные DNS-серверы для домена.

## 2. Трассировка маршрута

Команда traceroute usm.md показала путь из локальной сети до хостинга ресурса:

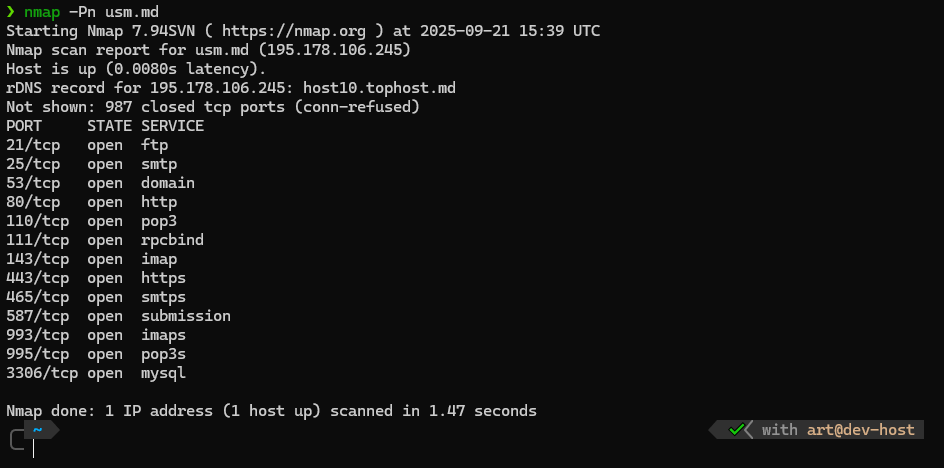
1. Локальный шлюз (192.168.0.1)
2. Первый hop у провайдера (192.0.0.1) 3–5. Узлы провайдера net.md (77.89.192.\* и 172.30.192.\*)
3. Магистральный провайдер AS15836 (ARAX) 7–9. Промежуточные маршрутизаторы (10.89.4.25, 185.212.9.1, 195.178.106.1)
4. Конечный сервер: host10.tophost.md (195.178.106.245)

Таким образом, маршрут включает локальную сеть, национальный сегмент net.md, транзит через ARAX (IXP) и выход на хостинг-провайдера.



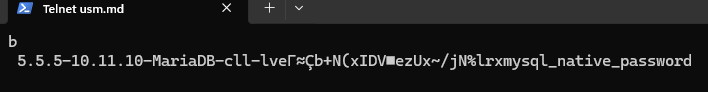
## 3. Сканирование портов (Nmap)

Сканирование с помощью nmap -Pn usm.md показало следующие открытые TCP-порты:



Можно сделать вывод о слабой защите серверной части. Большая площадь атаки, открыты порты начиная от необходимых (сетевых почтовых), заканчивая базой данных, ftp, rpc, порт dns.

telnet на порт 3306



Теперь я уже знаю что версия maria db 10.11.10, замаскированная под 5.5.5, возможно стоит cpanel.

Тем более используется mysql\_native\_password.

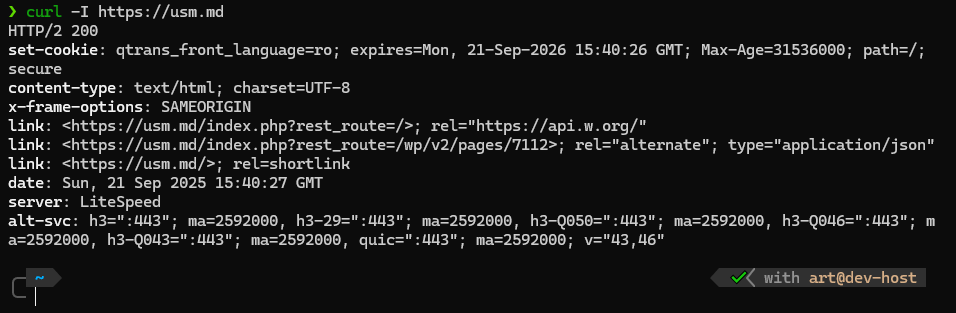
Думаю при желании кто то может получить доступ, но возможно это honeypot.

## 4. HTTP-заголовки

Запрос curl -I https://usm.md вернул ответ:

* Код состояния: 200 OK
* Сервер: LiteSpeed
* Применяются стандартные механизмы защиты: X-Frame-Options: SAMEORIGIN
* Подключены ссылки на WordPress API (/wp-json/).

Таким образом, сайт работает на CMS WordPress с веб-сервером LiteSpeed.



## 5. SSL-сертификат

Проверка через openssl s\_client -connect usm.md:443 показала:

* Сертификат выдан Let's Encrypt R11
* Доменное имя в сертификате: 75.usm.md
* Алгоритм: RSA 2048 бит, SHA-256
* Срок действия: 08.08.2025 – 06.11.2025
* Используется современный протокол TLS 1.3 и шифр TLS\_AES\_256\_GCM\_SHA384
* Проверка цепочки сертификатов прошла успешно (*Verify return code: 0*).

Таким образом, соединение с сайтом защищено и соответствует современным стандартам криптографии.

❯ openssl s\_client -connect usm.md:443

CONNECTED(00000003)

depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1

verify return:1

depth=1 C = US, O = Let's Encrypt, CN = R11

verify return:1

depth=0 CN = 75.usm.md

verify return:1

---

Certificate chain

0 s:CN = 75.usm.md

i:C = US, O = Let's Encrypt, CN = R11

a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256

v:NotBefore: Aug 8 20:44:03 2025 GMT; NotAfter: Nov 6 20:44:02 2025 GMT

1 s:C = US, O = Let's Encrypt, CN = R11

i:C = US, O = Internet Security Research Group, CN = ISRG Root X1

a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256

v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT

---

Server certificate

-----BEGIN CERTIFICATE-----

MIIFfzCCBGegAwIBAgISBntFNL2lzyJIrXwP2j/yVJ4wMA0GCSqGSIb3DQEBCwUA

MDMxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQwwCgYDVQQD

EwNSMTEwHhcNMjUwODA4MjA0NDAzWhcNMjUxMTA2MjA0NDAyWjAUMRIwEAYDVQQD

Ewk3NS51c20ubWQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzXN8+

t+2VLZAn1eoBxGYcLZNdFLP5Uidx/v4+43GETtzg1tfeQQAk8DGh4a3mISFk2oam

IK8+XcBBsWURCswRfIG3YefCQE4+94UnyvQDq2FmsndwmGvRa2VhFPTdNASv0Vug

k++murvdnFPfvpa8gRiz4MxOoGZ/+rZVCsUl2bQIyrSrjsdTE2cSM/tu2OteUwmh

K6lpZzVdy3JKMn9CKuBCH81nEW/zadKiwpot++mUubjc6RCkrUE855OvVtmvWHa4

Pc2vA0BDBR3llUdyH0m5g2UMQe3+eMei97ebHgsGZPJ/85NTjilRWwQS1Mi7IWvw

HlQM5MyvhVdqABrTAgMBAAGjggKqMIICpjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0l

BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYE

FHZ+bSJthYK0m1M+OHW5m1oc7CJiMB8GA1UdIwQYMBaAFMXPRqTq9MPAemyVxC2w

XpIvJuO5MDMGCCsGAQUFBwEBBCcwJTAjBggrBgEFBQcwAoYXaHR0cDovL3IxMS5p

LmxlbmNyLm9yZy8wgaQGA1UdEQSBnDCBmYIJNzUudXNtLm1kgg9hZG1pdGVyZS51

c20ubWSCDGFzdXNtLnVzbS5tZIINY2hpbWllLnVzbS5tZIINZXVmb3J5LnVzbS5t

ZIINZnJpc3BhLnVzbS5tZIIKZnNlLnVzbS5tZIIQanVybmFsaXNtLnVzbS5tZIIN

bGl0ZXJlLnVzbS5tZIILcGh5cy51c20ubWSCBnVzbS5tZDATBgNVHSAEDDAKMAgG

BmeBDAECATAuBgNVHR8EJzAlMCOgIaAfhh1odHRwOi8vcjExLmMubGVuY3Iub3Jn

LzQ5LmNybDCCAQQGCisGAQQB1nkCBAIEgfUEgfIA8AB1AKRCxQZJYGFUjw/U6pz7

ei0mRU2HqX8v30VZ9idPOoRUAAABmIuiuHgAAAQDAEYwRAIgf6gMH2AtcG+7fqdZ

bUhJLRUQaibTl6UY+rz2puNYSPYCIFSPCf84k76pFRjlpLO9d97LryeaBgxtU+Wf

EHdf7a6aAHcA3dzKNJXX4RYF55Uy+sef+D0cUN/bADoUEnYKLKy7yCoAAAGYi6K4

wwAABAMASDBGAiEAh/anN1RTtLQBqapADNA+HNMfSnZz/9cYUOMlWUjRMlICIQDM

WZBoaL80zASVGNODniYSLoa/gMyrsdBNjRtoeXuckzANBgkqhkiG9w0BAQsFAAOC

AQEAb+SBvh2JrQxTHHp6MBP/kDidOvqOhNyiCRvMRLPXE7V0mCo386jOeo48we6r

9IUjV5hAU9SWjbuqYpVy4sYmYmYuAqbNw2mOiJPkD4IclqdBk8+brfyp0CDHVBBb

Mkr9vzHLtm2GszCeeyNUif622gwSuEb2ZTAJH8eG2F3WF5aHSHwLyzCZltzB/qtT

pfsX0NM65yLURpyLJFWXfl/6g/Hfzg2uo2f+QFEG05v7D20THQMh6prvgbZEf+6g

k9nGdmmwCYiTjZFPqMxD2B6Su+3IB3AAco4tjQzeky0aunMpIcxhWz87IRiyBvMc

RMyl/XQV0fZBoy1GJiYHdGzH1Q==

-----END CERTIFICATE-----

subject=CN = 75.usm.md

issuer=C = US, O = Let's Encrypt, CN = R11

---

No client certificate CA names sent

Peer signing digest: SHA256

Peer signature type: RSA-PSS

Server Temp Key: X25519, 253 bits

---

SSL handshake has read 3196 bytes and written 388 bytes

Verification: OK

---

New, TLSv1.3, Cipher is TLS\_AES\_256\_GCM\_SHA384

Server public key is 2048 bit

Secure Renegotiation IS NOT supported

Compression: NONE

Expansion: NONE

No ALPN negotiated

Early data was not sent

Verify return code: 0 (ok)

---

---

Post-Handshake New Session Ticket arrived:

SSL-Session:

Protocol : TLSv1.3

Cipher : TLS\_AES\_256\_GCM\_SHA384

Session-ID: 810AF874622F34FA8122B09E54A0168D26BD8DCAFD7010C28C5AAC6234850A32

Session-ID-ctx:

Resumption PSK: BE06AF7D43AF4382FA391C4D3D829E8DC42D7BF30635EE39E6283835FD052F16C107D0F7584C8EDFCDFA922EF51FC09C

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 172800 (seconds)

TLS session ticket:

0000 - b8 9f af 5c 7a ad 53 6e-03 4b 57 c3 e0 c0 b2 f1 ...\z.Sn.KW.....

0010 - d4 d2 98 97 c2 8f 05 ba-a2 94 e7 bf 58 b3 8e 34 ............X..4

0020 - b9 b2 74 22 c2 19 de 08-f6 a1 a9 dd 52 bc 58 3d ..t"........R.X=

0030 - b7 3c ce 1d fb 56 b6 4a-da 08 bd 1c fe f3 51 86 .<...V.J......Q.

0040 - c9 9f c0 73 04 71 01 42-37 c4 50 8f 7e b6 3c 37 ...s.q.B7.P.~.<7

0050 - c7 74 18 2b 11 2a 95 65-06 11 0a 87 cd 52 e0 a0 .t.+.\*.e.....R..

0060 - 42 e9 c5 86 63 3a 23 28-db 79 de a5 7d 62 9c 5b B...c:#(.y..}b.[

0070 - 6f ca 04 1d e8 99 fc 3a-c2 9a f6 68 ee 3c d2 70 o......:...h.<.p

0080 - db 7c 65 5d 52 80 35 9a-b7 1c 05 04 d1 95 4f 19 .|e]R.5.......O.

0090 - a4 ac c4 03 24 3d 25 49-66 92 9e 4e 69 53 d0 40 ....$=%If..NiS.@

00a0 - 66 30 e2 1e 9b 82 07 28-f4 af 90 74 ec 9a c6 72 f0.....(...t...r

00b0 - ce 1a b7 19 e9 38 ef e3-c8 b2 ea d7 76 9d 09 22 .....8......v.."

Start Time: 1758469274

Timeout : 7200 (sec)

Verify return code: 0 (ok)

Extended master secret: no

Max Early Data: 0

---

read R BLOCK

---

Post-Handshake New Session Ticket arrived:

SSL-Session:

Protocol : TLSv1.3

Cipher : TLS\_AES\_256\_GCM\_SHA384

Session-ID: A94C684DB12EE87CEC8E838857F4AB974C0776162881E070D9A71944E3F9D0DA

Session-ID-ctx:

Resumption PSK: 417BDF74141F63064B3C7D54E41B541746835805186EF9D1E43E3FA99F0A9EEECB02F866FA2CF3A3BF3F7B3383FFC77D

PSK identity: None

PSK identity hint: None

SRP username: None

TLS session ticket lifetime hint: 172800 (seconds)

TLS session ticket:

0000 - b8 9f af 5c 7a ad 53 6e-03 4b 57 c3 e0 c0 b2 f1 ...\z.Sn.KW.....

0010 - 6f db ca 6a b8 69 19 0c-32 fc 86 a5 47 7e b0 00 o..j.i..2...G~..

0020 - 38 ea ad f1 e4 5e 83 c2-40 3b 44 63 60 75 3e b5 8....^..@;Dc`u>.

0030 - 88 09 20 d1 45 78 78 55-84 38 86 03 a1 de b5 3e .. .ExxU.8.....>

0040 - b2 9f cd ae 28 9f c3 3c-fb dc 08 e5 04 ca e6 37 ....(..<.......7

0050 - 63 9b 98 3f a1 72 8f b9-f7 48 1f ae b2 41 6f 8f c..?.r...H...Ao.

0060 - 4d ec 3d 62 e1 8f 38 31-6c 5c 5f 3e 4d f4 98 d0 M.=b..81l\\_>M...

0070 - 08 c0 2a 63 c2 09 7f dc-18 85 46 61 0e cc b2 36 ..\*c......Fa...6

0080 - 91 82 26 ad 46 87 98 be-25 82 41 3f 43 fa 61 ab ..&.F...%.A?C.a.

0090 - 9b 44 6b 91 c5 33 c5 08-86 99 b9 76 5c 3c dd b9 .Dk..3.....v\<..

00a0 - 3a 8c f7 e5 d0 b4 a2 1b-c8 0c 07 98 ae c1 05 33 :..............3

00b0 - 04 15 a1 3a 04 7d 21 28-47 1b 40 f7 d2 4e 06 07 ...:.}!(G.@..N..

Start Time: 1758469274

Timeout : 7200 (sec)

Verify return code: 0 (ok)

Extended master secret: no

Max Early Data: 0

---

read R BLOCK

closed

# Часть 4: Контрольные вопросы

## **1. Частные vs публичные IP:**

Частные (например 192.168.x.x, 10.x.x.x, 172.16–31.x.x) — используются внутри локальных сетей, в интернет напрямую не маршрутизируются.

Публичные — уникальные адреса, видимые в интернете, через них доступен ресурс.

## **2. Для чего нужны порты:**

Порт = «дверь» в системе, которая привязана к процессу/сервису.

TCP и UDP используют порты, чтобы разделять разные приложения (например, 80 — HTTP, 443 — HTTPS, 22 — SSH).

Без портов невозможно было бы понять, какому процессу доставить пакет.

## **3. Как работает DNS:**

DNS = «телефонная книга интернета».

Введенное доменное имя отправляется на резолвер - резолвер спрашивает у DNS-сервера - идёт цепочка запросов (root - TLD - авторитетный сервер).

В итоге возвращается IP-адрес (A/AAAA-запись) или другая запись (MX, CNAME и т.д.).

## **4. Как проверить, открыт ли порт:**

* nmap (самый удобный):

nmap -p 80 example.com

* nc (netcat):

nc -vz example.com 80

* telnet (старый способ):

telnet example.com 80