Мельникова А.С. ИВТ 3 курс группа 1.2

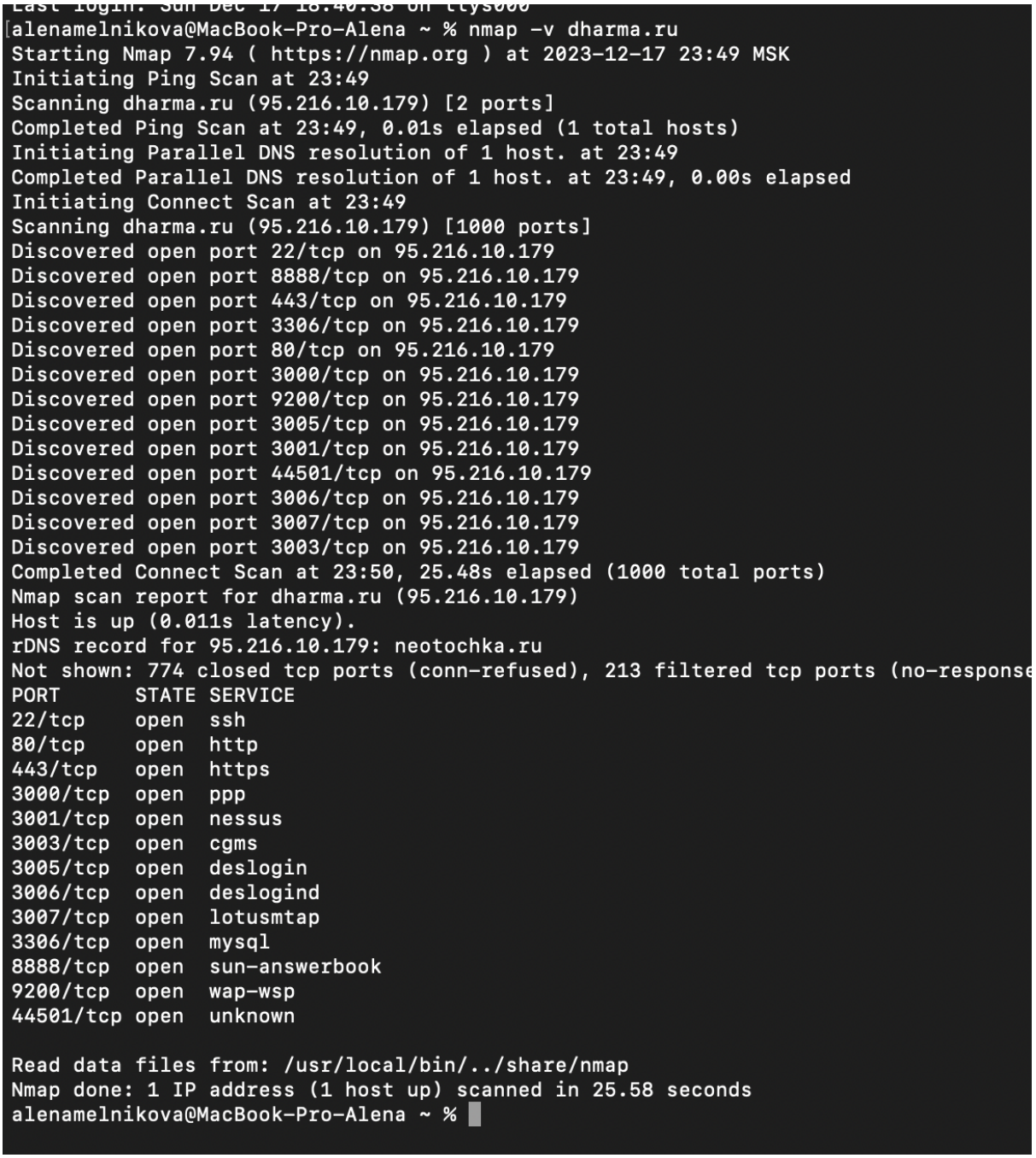
Использование netstat:

Активные подключения(что то очень много……):

```
Nmap done: 1 IP address (1 host up) scanned in 42.51 seconds
alenamelnikova@MacBook-Pro-Alena ~ % netstat
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  192.168.0.102.59343    149.154.167.35.https   ESTABLISHED
tcp4       0      0  192.168.0.102.59341    srv209-185-240-8.https ESTABLISHED
tcp4       0      0  192.168.0.102.59340    lh-in-f94.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59339    lm-in-f113.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59338    lg-in-f84.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59337    lf-in-f157.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59335    lq-in-f94.1e100..https ESTABLISHED
[tcp4      0      0  192.168.0.102.59334    lu-in-f94.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59333    mc.yandex.ru.https     ESTABLISHED
tcp4       0      0  192.168.0.102.59332    lt-in-f101.1e100.https ESTABLISHED
tcp6       0      0  macbook-pro-alen.1024  fe80::2807:b30a:.1024  SYN_SENT
tcp4       0      0  192.168.0.102.59330    lt-in-f139.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59329    srv90-190-240-87.https ESTABLISHED
tcp4       0      0  192.168.0.102.59317    srv90-190-240-87.https ESTABLISHED
tcp4       0      0  192.168.0.102.59316    lf-in-f100.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59315    lt-in-f104.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59314    lg-in-f102.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59313    lg-in-f102.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59312    lu-in-f84.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59310    149.154.167.35.https   ESTABLISHED
tcp4       0      0  192.168.0.102.59309    149.154.167.35.https   ESTABLISHED
tcp4       0      0  192.168.0.102.59308    149.154.167.35.https   ESTABLISHED
tcp4       0      0  192.168.0.102.59307    149.154.167.35.https   ESTABLISHED
tcp4       0      0  192.168.0.102.59305    la-in-f95.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59301    lg-in-f95.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59300    srv208-185-240-8.https ESTABLISHED
tcp4       0      0  192.168.0.102.59295    srv90-190-240-87.https ESTABLISHED
tcp4       0      0  192.168.0.102.59294    149.154.167.255.https  ESTABLISHED
tcp4       0      0  192.168.0.102.59293    149.154.167.255.https  ESTABLISHED
tcp4       0      0  192.168.0.102.59283    srv200-185-240-8.https ESTABLISHED
tcp4       0      0  192.168.0.102.59263    lh-in-f94.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59262    lu-in-f138.1e100.https ESTABLISHED
tcp4       0      0  192.168.0.102.59261    lj-in-f95.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59259    lj-in-f95.1e100..https ESTABLISHED
tcp4       0      0  192.168.0.102.59258    srv186-129-240-8.https ESTABLISHED
tcp4       0      0  192.168.0.102.59227    srv199-185-240-8.https ESTABLISHED
tcp4       0      0  192.168.0.102.59224    srv132-129-240-8.https ESTABLISHED
tcp4       0      0  192.168.0.102.59221    srv72-132-240-87.https ESTABLISHED
tcp4       0      0  192.168.0.102.59208    log.strm.yandex..https ESTABLISHED
tcp4       0      0  192.168.0.102.59195    adfox-external-l.https ESTABLISHED
tcp4       0      0  192.168.0.102.59169    yandex.ru.https        ESTABLISHED
tcp4       0      0  192.168.0.102.59142    srv72-132-240-87.https ESTABLISHED
tcp4       0      0  192.168.0.102.57049    yandex.ru.https        ESTABLISHED
tcp4       0      0  192.168.0.102.57022    149.154.167.50.https   ESTABLISHED
tcp4       0      0  192.168.0.102.56974    yandex.ru.https        ESTABLISHED
tcp4       0      0  192.168.0.102.56972    forms-public-www.https ESTABLISHED
tcp4       0      0  192.168.0.102.56865    core-renderer-ti.https ESTABLISHED
tcp4       0      0  192.168.0.102.56862    front-jsapi.slb..https ESTABLISHED
tcp4       0      0  192.168.0.102.56802    adfox-external-l.https ESTABLISHED
tcp4       0      0  192.168.0.102.56781    yandex.ru.https        ESTABLISHED
tcp4       0      0  192.168.0.102.56756    yandex.ru.https        ESTABLISHED
tcp4       0      0  192.168.0.102.56721    adfox-external-l.https ESTABLISHED
tcp4       0      0  192.168.0.102.56716    yandex.ru.https        ESTABLISHED
tcp4       0      0  192.168.0.102.54886    grampus-server.r.https ESTABLISHED
tcp4       0      0  192.168.0.102.54760    bs.yandex.ru.https     ESTABLISHED
tcp4       0      0  192.168.0.102.53008    149.154.167.50.https   ESTABLISHED
tcp6       0      0  macbook-pro-alen.52786 iphone.59607           ESTABLISHED
tcp4       0      0  192.168.0.102.52787    lu-in-f188.1e100.5228  ESTABLISHED
tcp4       0      0  192.168.0.102.55692    17.248.214.64.443      TIME_WAIT
```

Использование nmap:

Я решила просканировать порты сайта буддийского интернет-магазина dharma.ru :



Из того что я увидела:

22 порт: SSH по умолчанию работает на порту 22
80 порт: http :)

443 порт: https :)
3000 порт: PPP Протокол PPP подразумевает физическое соединение двух систем по телефонной линии. Например, соединение PPP между сервером в филиале компании и сервером в центральном офисе позволяет передавать данные из одной системы в другую.
PPP позволяет взаимодействовать сетевому программному обеспечению от различных производителей. Кроме того, с его помощью несколько сетевых протоколов могут использовать одну линию связи.(информация из интернета)

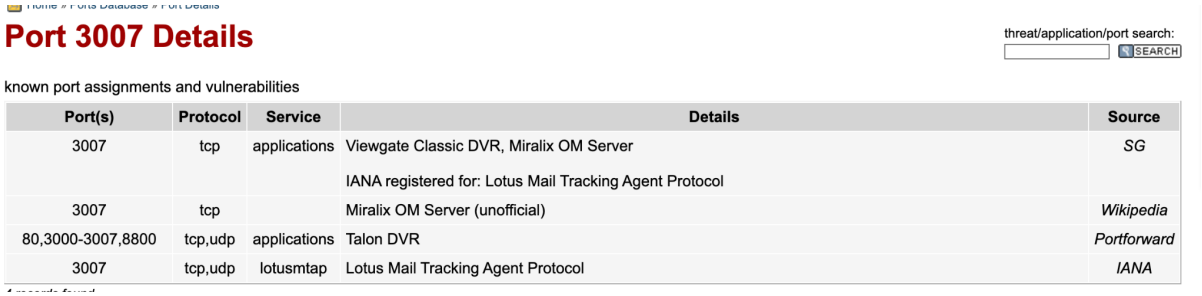
3001 порт: nessus Nessus — программа для автоматического поиска известных изъянов в защите информационных систем. Она способна обнаружить наиболее часто встречающиеся виды уязвимостей, например:

- Наличие уязвимых версий служб или доменов
- Ошибки в конфигурации (например, отсутствие необходимости авторизации на SMTP-сервере)
- Наличие паролей по умолчанию, пустых, или слабых паролей(wiki)

3003 порт: cgms ???? из того что нашла: CGMS чаще всего применяется в контексте защиты авторских прав на видеоматериалы, такие как фильмы или телепередачи. Тем не менее, в современных цифровых технологиях и стриминге контента могут использоваться другие методы защиты авторских прав, и CGMS в первую очередь связан с аналоговыми видеосигналами.

3005 и 3006 порт: … непонятно

3007 порт: lotusmtap найденная информация:



Port 3007 Details

threat/application/port search: SEARCH

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
3007	tcp	applications	Viewgate Classic DVR, Miralix OM Server	*SG*
			IANA registered for: Lotus Mail Tracking Agent Protocol	
3007	tcp		Miralix OM Server (unofficial)	*Wikipedia*
80,3000-3007,8800	tcp,udp	applications	Talon DVR	*Portforward*
3007	tcp,udp	lotusmtap	Lotus Mail Tracking Agent Protocol	*IANA*

3306 порт: mysql

Порт 3306 является стандартным портом для протокола MySQL, который является одной из самых популярных систем управления базами данных (СУБД). MySQL используется для хранения и управления данными, особенно в веб-приложениях.

8888 порт: sun answerbook Протокол Sun AnswerBook — это собственный протокол Sun Microsystems, используемый для доступа к онлайн-базе данных технической поддержки Sun, известной как AnswerBook.

9200 порт:

Wireless Application Protocol (WAP) и Wireless Session Protocol (WSP) являются частями технологий, предназначенных для обеспечения доступа к интернет-содержимому через мобильные устройства. В контексте порта 9200, который обычно используется для Elasticsearch, WAP и WSP, вероятно, не имеют отношения.(но здесь почему-то имеют)

44501 порт: unknown

Когда вы видите результат "44501 unknown" при сканировании портов, это означает, что сканер обнаружил открытый порт 44501, но не смог определить точное приложение или службу, которая использует этот порт.