Домашнее задание урок 5.

Используя netstat или ss исследовать 5 UDP и 5 TCP сокетов на вашей машине/виртуалке/сервере.

Команда: netstat -a -b -o -f -p TCP >> netstat_TCP

Результат в таблице:

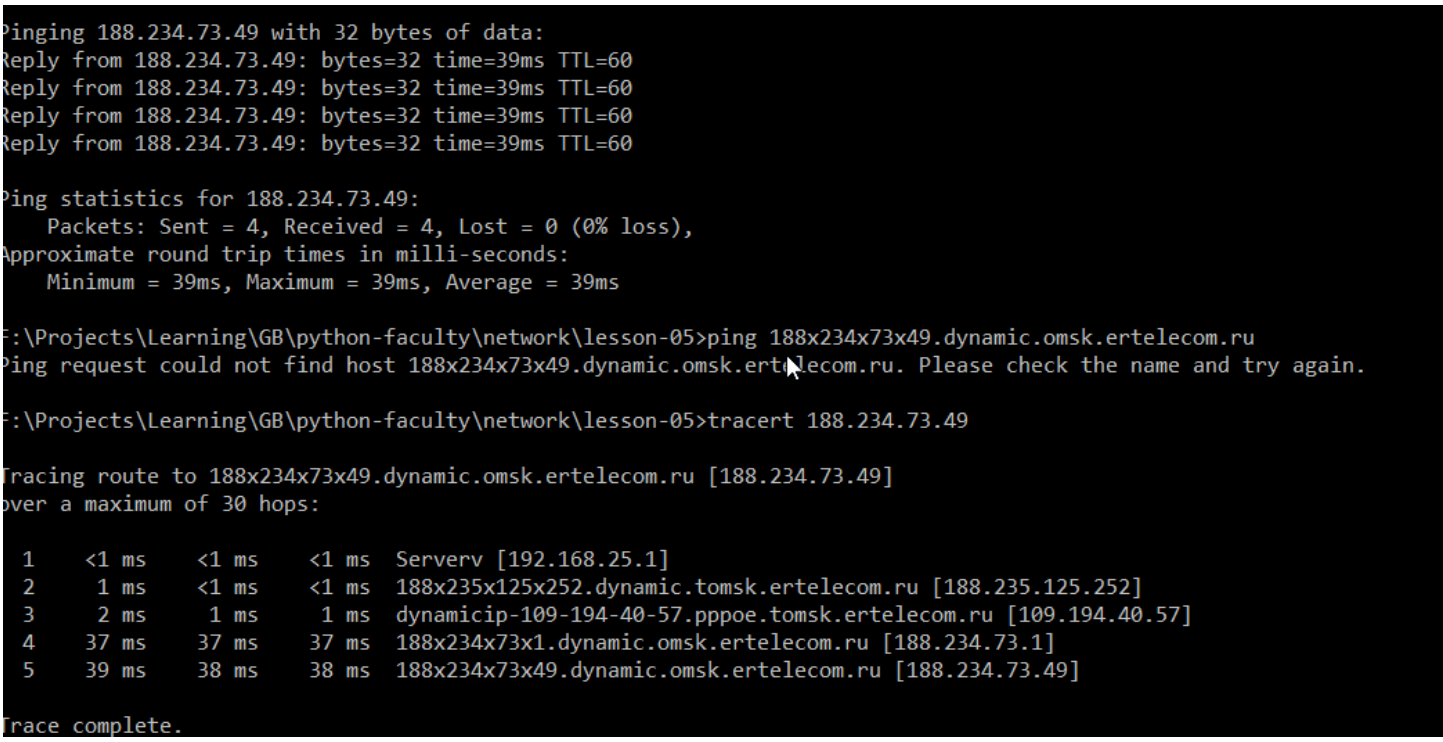
Active Connections

нпп	Proto (TCP)	Local Address	Foreign Address	State	PID
1	opera.exe	192.168.25.102:52268	yandex.ru:https	ESTABLISHED	3672
2	YandexDisk2.exe	192.168.25.102:59422	xiva-daria.stable.qloud-b.yandex.net:https	ESTABLISHED	10228
3	mstsc.exe	192.168.25.102:58590	Serverv:ms-wbt-server	ESTABLISHED	16440
4	Can not obtain ownership information	192.168.25.102:56718	WIN-01:microsoft-ds	ESTABLISHED	4
5	putty.exe	192.168.25.102:55366	192.168.25.108:ssh	ESTABLISHED	8896
6	SearchApp.exe	192.168.25.102:65373	188x234x73x49.dynamic.omsk.ertelecom.ru:https	CLOSE_WAIT	9360

Описание:

Мой локальный IP - 192.168.25.102.

1. Процесс опера, со случайного порта 52268 установил соединение с яндексом по порту 443.
2. Процесс яндекс диска, со случайного порта 59422 установил соединение с xiva-daria.stable.qloud-b.yandex.net по https, думаю он ожидает данные по синхронизаци
3. Процесс mstsc.exe, со случайного порта 58590 установил соединение с Serverv по порту 3389 (ms-wbt-server) это я подключился к своему шлюзу по RPD
4. Это интересней) почему-то netstat не может определить что это, если я все верно отыскал, то microsoft-ds (445 порт) это общий доступ к файлам и принтерам, вроде все сходится, WIN-01 это моя виртуальная машина (на hyper-v) там есть шара для обмена.
5. Процесс putty.exe, со случайного порта 55366, установил соединение с 192.168.25.108 по порту ssh, это моя защищенная сессия с сервером убунту.
6. Вот это самое непонятное, для начала адрес, днс не может его распознать, откуда он взялся не понимаю, если переключить netstat в режим показа адресов там будет: 188x234x73x49 (? Такое мы вроде не проходили), если пингануть 188.234.73.49, то пингуется, трассировка проходит нормально (скрин ниже) полагаю это шлюз провайдера. Само приложение - это служба поиска кортаны, ИИ windows 10. Далее состояние, тоже не однозначно, по розыскам в интернете состояние я сделал вывод, что состояние CLOSE_WAIT, которое долго висит, означает что локальное приложение закрывает сокет. И вот вопрос: зачем кортане это подключение? Я не знаю, наверное она за мной следит). Но я ее собирался выпилить и так.



Команда: netstat -a -b -o -f -p UDP >> netstat_UDP

Результат в таблице:

Active Connections

нпп	Proto (UDP)	Local Address	Foreign Address	State	PID
1	SharedAccess svchost.exe	0.0.0.0:53	*:*		3024
2	opera.exe	0.0.0.0:5353	*:*		15808
3	steam.exe	0.0.0.0:27036	*:*		12676
4	dashost.exe	0.0.0.0:3702	*:*		4488
5	SSDPSRV	172.25.96.1:1900	*:*		5000

Описание:

Если я верно все понимаю, то никакого соединения в случае UDP нет, сервис просто слушает какой-то порт, в надежде что-то получить.

1. Это DNS, системная служба svchost, принимает запросы на разрешение имен адресов, думаю так. Что есть “SharedAccess”, применительно к netstat мне не удалось понять, может вы расскажите на уроке.
2. Оказалось, что это порт мультикаста DNS, зачем опера его слушает не ясно, поиск в инете показал, я не один не понимаю зачем, советуют его закрыть)
3. Клиент стим на порту 27036, стим много чего делает, думаю это входящие трансляции, по материалам урока это лучше всего подходит
4. dashost.exe - это Device Association Framework Provider Host является основой для подключения и сопряжения проводных и беспроводных устройств с Windows, полагаю что ожидает данные об устройстве, которое хочет подключиться к моей машине.
5. SSDPSRV - Простой протокол обнаружения сервисов (англ. Simple Service Discovery Protocol, SSDP) работает на порту 1900, согласуется с документаций, 172.25.96.1 это адрес моей виртуальной машины (но интерфейс он

на моей локальной машине) на винде, а с убунту такого соединения нет, думаю это фича виндовс, сам хост рассылает информацию о своих простых сервисах, а служба их регистрирует и ожидает информации.