



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего
образования

РТУ МИРЭА

«МИРЭА – Российский технологический университет»

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»

Практическая работа № 2

«Основы безопасности ОС Windows»

по дисциплине «Безопасность операционных систем»

Москва

2023

2.1. Политики безопасности Windows

Политики параметров безопасности — это правила, которые можно настроить на устройстве или нескольких устройствах для защиты ресурсов на устройстве или в сети. Подробнее о политиках безопасности Вы можете прочитать здесь: [«https://learn.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/administer-security-policy-settings»](https://learn.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/administer-security-policy-settings).

Мы подробнее познакомимся с политиками безопасности учетных записей. Для открытия оснастки управления политиками безопасности в окне поиска windows (внизу рабочего стола иконка с лупой) или в окне выполнения команд (Win + r) введите `secpol.msc`, должно открыться окно как на рисунке 1.

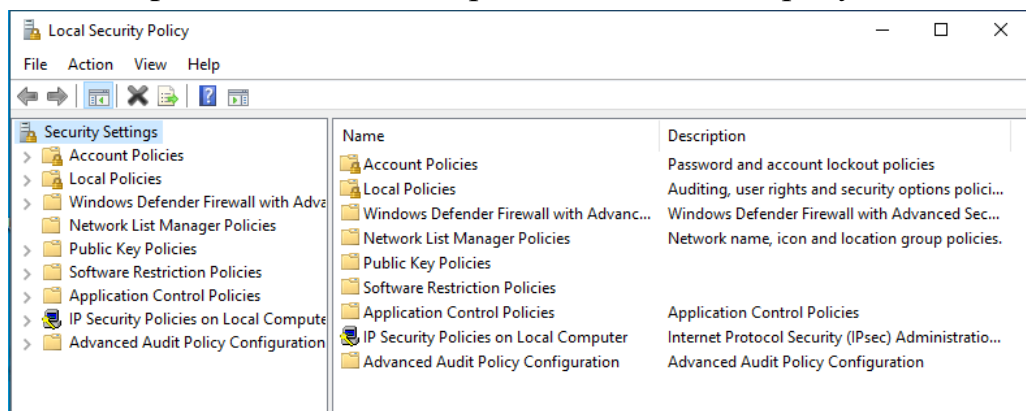


Рисунок 1. Окно оснастки локальных политик безопасности

Теперь перейдем в *Account Policies* -> *Account Lockout Policies* и выполним настройку параметров блокировки пользователя, как показано на рисунке 2.

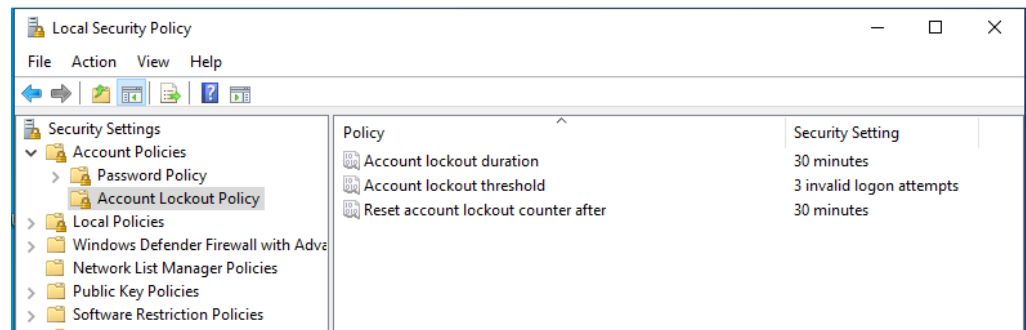


Рисунок 2. Параметры блокировки пользователей

Отчёт:

- Запишите в отчет, что означают данные параметры.
- Добейтесь блокировки пользователя (screenshot).
- Выполните настройку политики паролей (screenshot).
- Создайте нового пользователя с именем baso-0*-21-family, задайте ему пароль (screenshot).

Рассмотрим еще немного фич безопасности от политик. По умолчанию, на заблокированном экране или при запуске ОС, отображаются имена пользователей ОС, как показано на рисунке 3, что может быть полезно для злоумышленника.

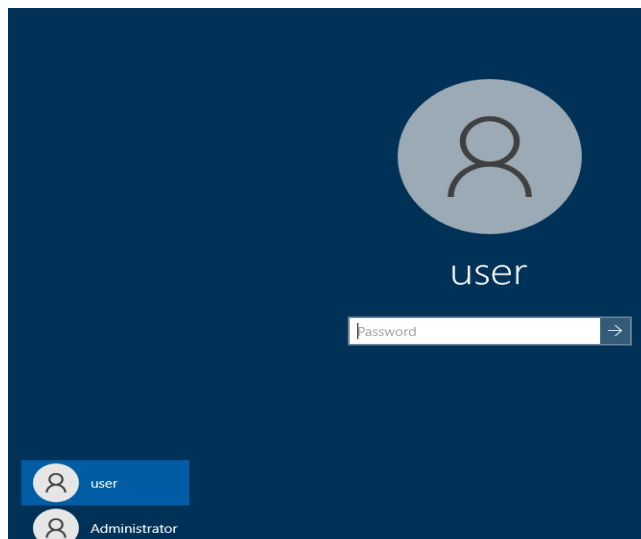


Рисунок 3. Окно авторизации Windows

Давайте скроем их запусив оснастку *secpol.msc* и перейдя в ветку *Local Policies -> Security Options*, включите параметры *Interactive logon: Don't display last signed-in* и установив значение параметра *Interactive logon: Display User Information when the session is locked* в *Do not display user information*. Результат на рисунке 4.

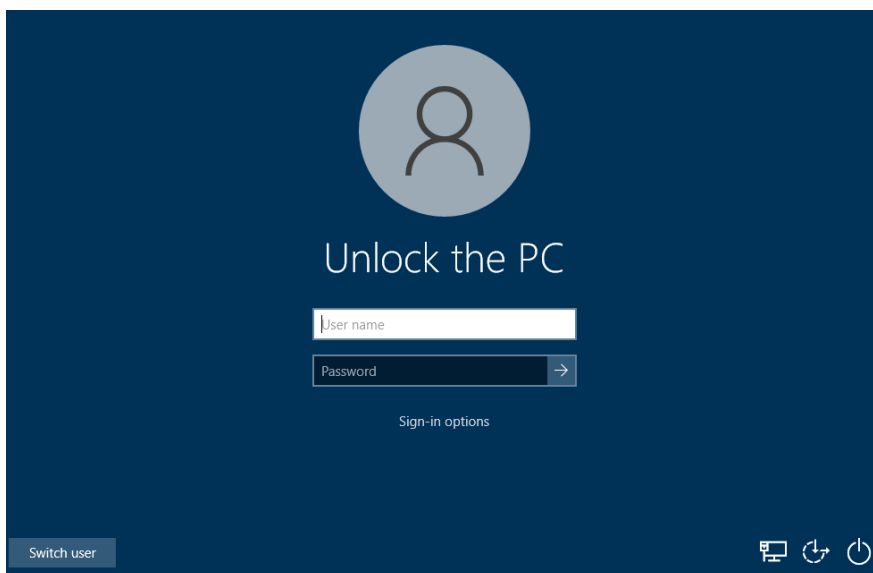


Рисунок 4. Окно авторизации Windows, пользователи скрыты

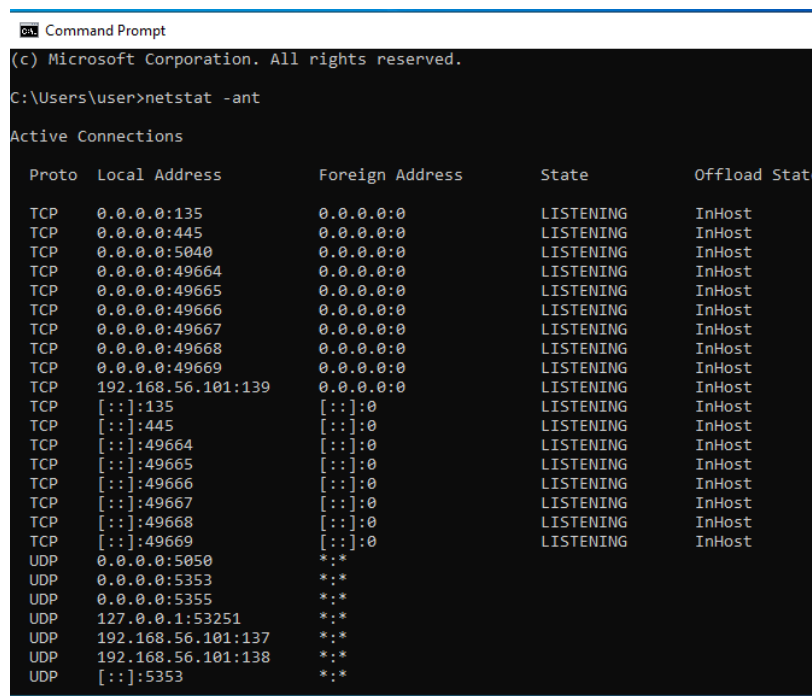
Отчёт:

- Занесите снимки экрана авторизации до и после отключения отображения пользователей в политиках безопасности (screenshot).

2.2. Брандмауэр Защитника Windows

Брандмауэр Защитника Windows в режиме повышенной безопасности обеспечивает двустороннюю фильтрацию сетевого трафика на основе узла и блокирует несанкционированный сетевой трафик, поступающий на локальное устройство или из него. Подробнее о настройке брандмауэра Вы можете прочитать здесь: [«https://learn.microsoft.com/ru-ru/windows/security/operating-system-security/network-security/windows-firewall/best-practices-configuring»](https://learn.microsoft.com/ru-ru/windows/security/operating-system-security/network-security/windows-firewall/best-practices-configuring).

Давайте посмотрим на потенциально уязвимые места ОС, защитником которых является брандмауэр. Выполните команду `netstat -ant`, как показано на рисунке



```
Command Prompt
(c) Microsoft Corporation. All rights reserved.
C:\Users\user>netstat -ant

Active Connections

Proto Local Address           Foreign Address         State       Offload State
TCP    0.0.0.0:135              0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:445              0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:49664            0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:49665            0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:49666            0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:49667            0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:49668            0.0.0.0:0               LISTENING   InHost
TCP    0.0.0.0:49669            0.0.0.0:0               LISTENING   InHost
TCP    192.168.56.101:139       0.0.0.0:0               LISTENING   InHost
TCP    [::]:135                 [::]:0                  LISTENING   InHost
TCP    [::]:445                 [::]:0                  LISTENING   InHost
TCP    [::]:49664               [::]:0                  LISTENING   InHost
TCP    [::]:49665               [::]:0                  LISTENING   InHost
TCP    [::]:49666               [::]:0                  LISTENING   InHost
TCP    [::]:49667               [::]:0                  LISTENING   InHost
TCP    [::]:49668               [::]:0                  LISTENING   InHost
TCP    [::]:49669               [::]:0                  LISTENING   InHost
UDP    0.0.0.0:5050             *:*                      LISTENING   InHost
UDP    0.0.0.0:5353             *:*                      LISTENING   InHost
UDP    0.0.0.0:5355             *:*                      LISTENING   InHost
UDP    127.0.0.1:53251          *:*                      LISTENING   InHost
UDP    192.168.56.101:137      *:*                      LISTENING   InHost
UDP    192.168.56.101:138      *:*                      LISTENING   InHost
UDP    [::]:5353                *:*                      LISTENING   InHost
```

Все строки, в которых поле State имеет значение LISTENING являются потенциальными местами компрометации ОС удаленными злоумышленниками.

Выполним следующее практическое задание. По умолчанию в Windows брандмауэр настроен на блокировку трафика, в этом можно убедиться «пропинговав» нашу ВМ, но для этого необходимо подготовиться:

1. Перевести режим работы сетевого адаптера в настройках виртуальной машины в сетевой мост, как показано на рисунке 5, для того чтобы наша виртуальная машина была доступна по сети с хостовой системы.

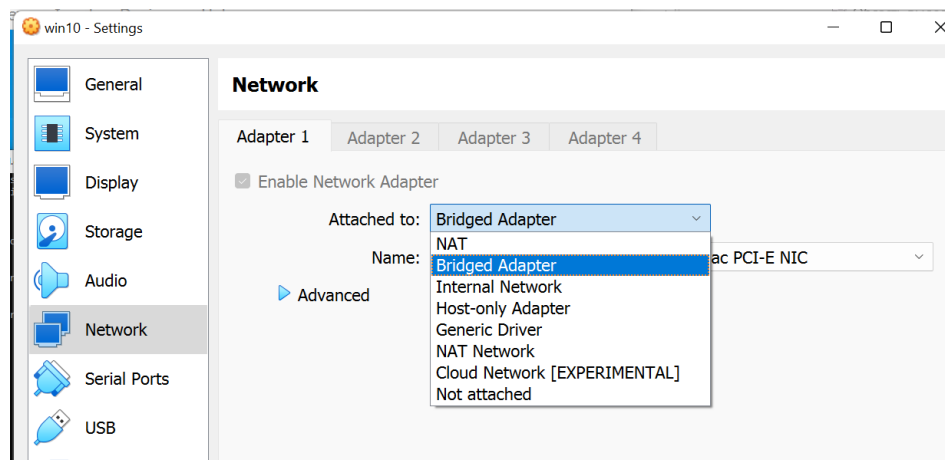


Рисунок 5. Настройки сетевого адаптера ВМ

2. Командой *ipconfig* Узнать ip-адрес ВМ и хостовой системы, как показано на рисунке 6.

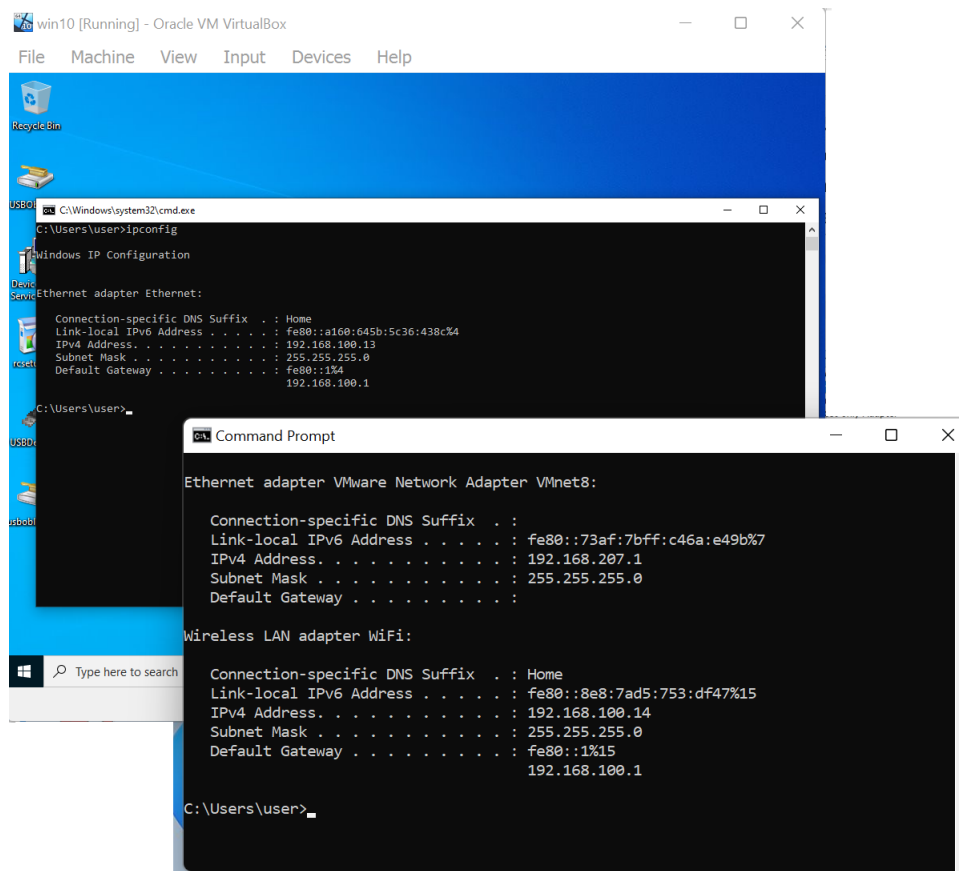


Рисунок 6. Результат команды *ipconfig*

3. Командой *ping* «пропинговать» обе системы, как показано на рисунке 7, результат будет отрицательный.

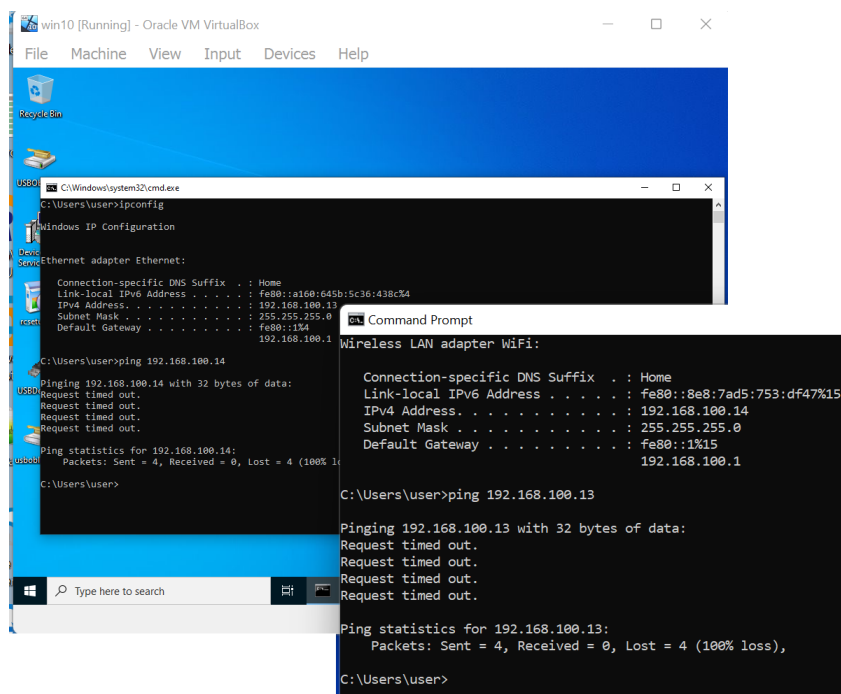


Рисунок 7. Результат команды ping

Теперь давайте настроим брандмауэр так, чтобы команда *ping* заработала. В окне поиска windows (внизу рабочего стола иконка с лупой) пишем *firewall*, из предложенных вариантов выбираем *Windows defender firewall with advanced security* откроется оснастка управления брандмауэром, как на рисунке 8.

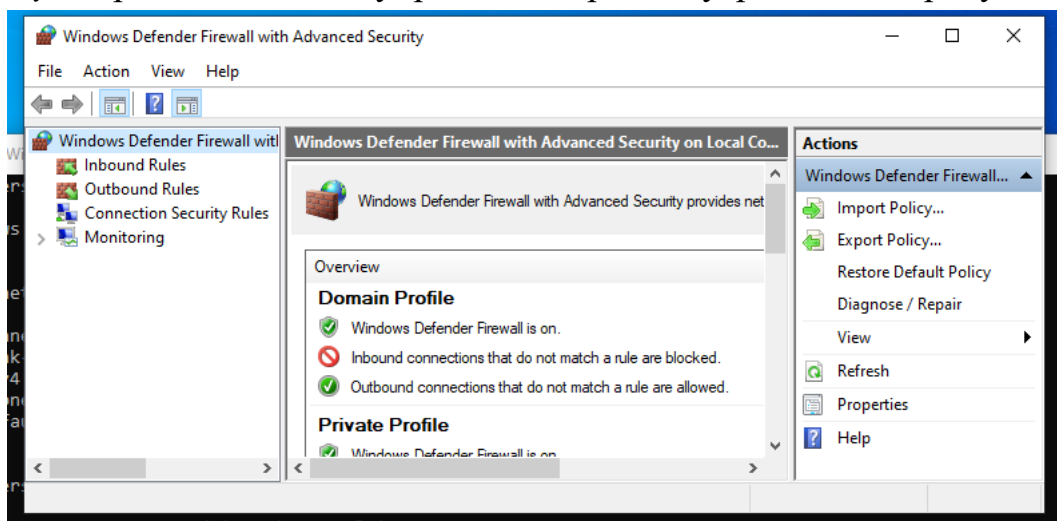


Рисунок 8. Оснастка управления брандмауэром

Перейдем в ветку *Inbound Rules* и выберем параметр *Core Networking Diagnostics – ICMP Echo Request (ICMPv4-IN)*, его надо включить, установив чекбокс *Enabled*, как показано на рисунке 9.

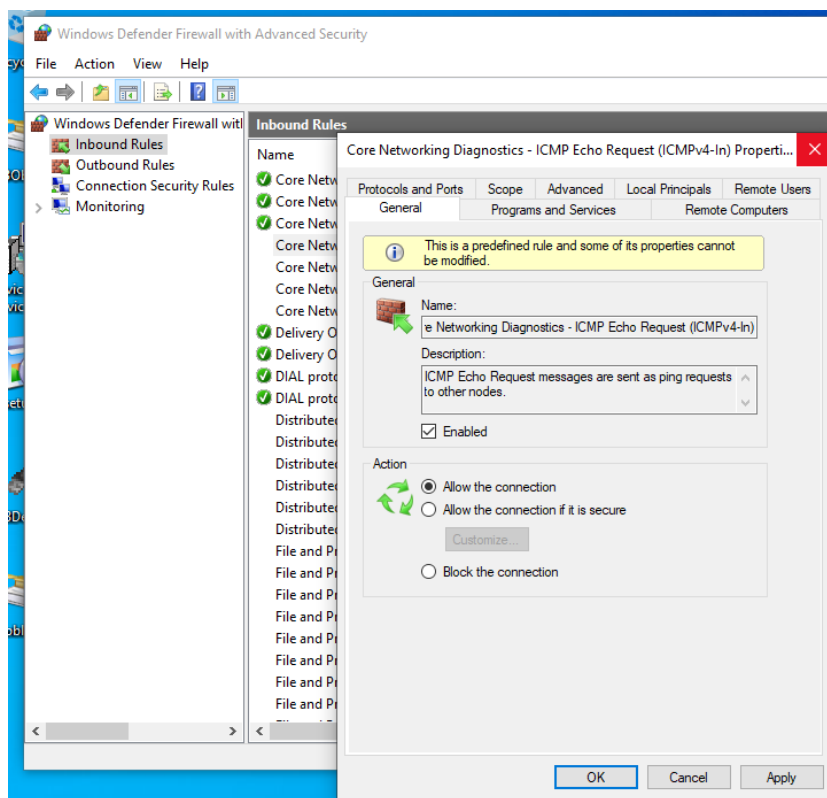


Рисунок 9. Включение параметра брандмауэра

Теперь еще раз «пропингуем» виртуальную и хостовую системы, получим результат, как на рисунке 10.

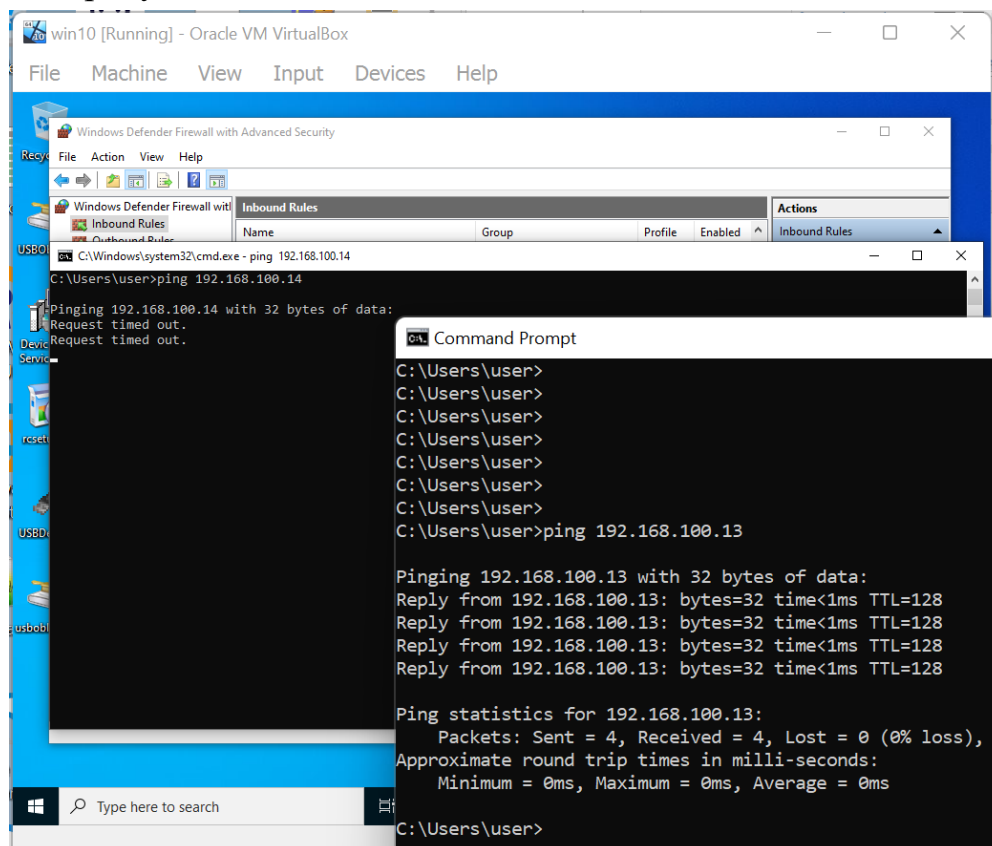


Рисунок 10. Результат команды ping

Отчёт:

- Объясните, почему получен результат, показанный на рисунке 10.
- Какой протокол используется командой ping и на каком уровне модели OSI он работает? (screenshot)
- Создайте собственное правило брандмауэра для блокировки протокола, который использует команда ping, только для ip-адреса вашей хостовой системы (screenshot).

2.3. Журналирование в Windows

Журналирование (протоколирование) - сбор и накопление информации о событиях, происходящих в информационной системе.

События бывают внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов), например, такие:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа и статуса объектов доступа
- и т. д.

Запуск оснастки журнала безопасности выполняется посредством команды `eventvwr.msc` в окне поиска windows (внизу рабочего стола иконка с лупой), окно оснастки показано на рисунке 11.

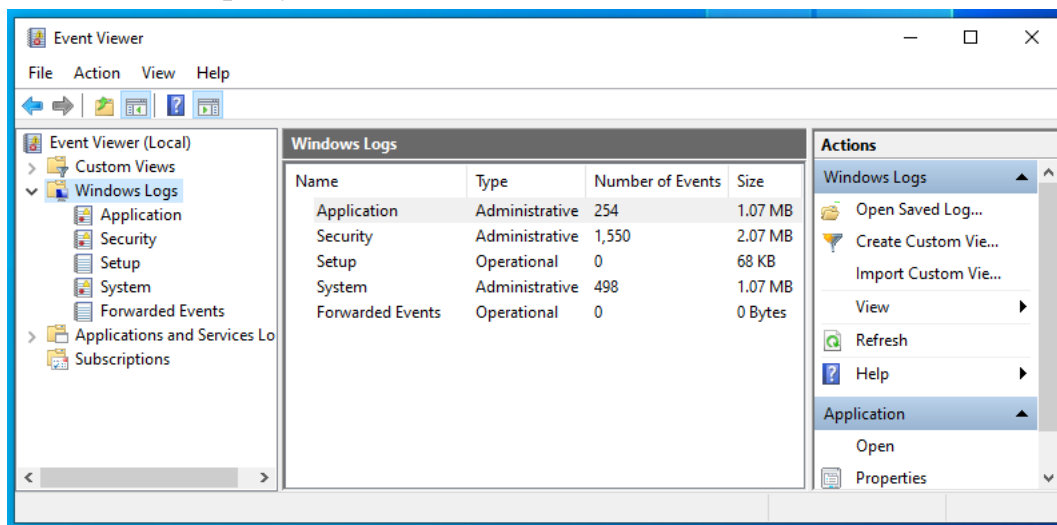


Рисунок 11 Окно оснастки журнала событий Windows

Воспользуемся фильтром и отобразим все события успешного входа в систему, код события 4624. В оснастке выбираем журнал *Security*, дальше в столбце *Action* выбираем *Filter Current Log* в открывшемся окне в поле *ID* вписываем код события, как показано на рисунке 12.

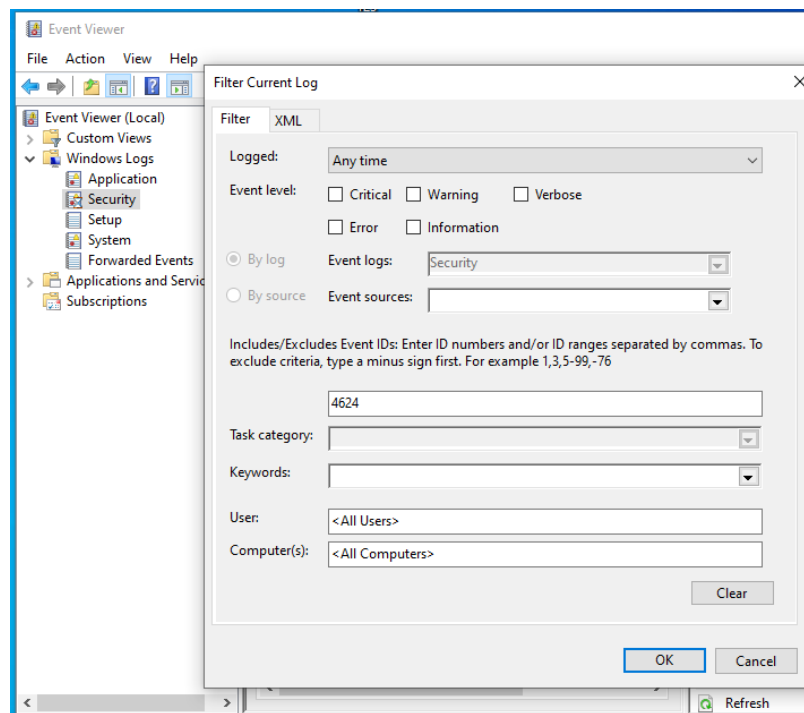


Рисунок 12 Фильтр журнала событий по коду

Отчёт:

- Найдите все события, связанные с неуспешным входом пользователя в систему (screenshot).
- Напишите в каких случаях обращаются к журналам событий Windows.
- Напишите ПО, которое применяется специалистами по ИБ для работы с журналами событий Windows.