Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Кафедра безпеки інформаційних систем та технологій

Лабораторна робота № 1

з навчальної дисципліни

«Захист інформації в інформаційно-комунікаційних системах»

Виконав:

Студент групи КБ-41

Кравченко Є.М.

Перевірив:

Доцент

Сватовський І.І.

Харків – 2021 р.

Тема: дослідження характеристик локальної мережі за допомогою утиліт ОС Linux.

Мета: навчитися досліджувати характеристики локальної мережі за допомогою утиліт ОС Linux.

**Хід роботи**

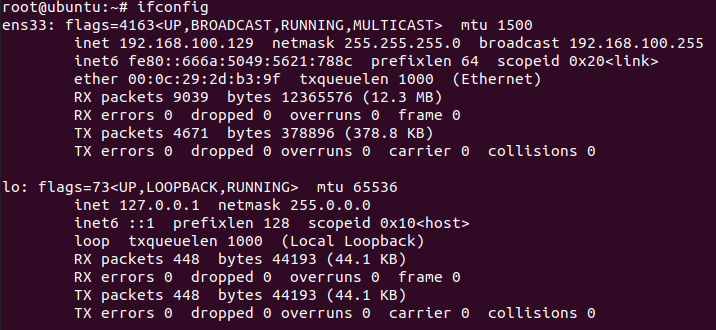
2. Зарегистрируйтесь в системе в первой консоли с правами администратора.



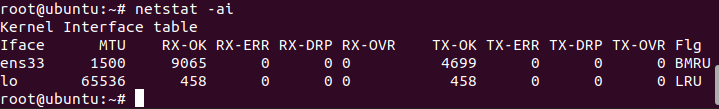
3. Зарегистрируйтесь во второй консоли с правами пользователя.



4. Из консоли администратора с помощью команды ifconfig -a выведите на экран данные о текущем состоянии всех сетевых интерфейсов компьютера. Какую информацию из прочитанного вывода вы извлекли? Запомните, как обозначается основной Ethernet-адаптер (он может обозначаться eth0, eth1, eth2), и в дальнейшем используйте в сетевых командах это имя. Далее в тексте задания он упоминается как eth0.



5. Выведите информацию о сетевых интерфейсах с помощью команды netstat –ai, сравните возможности двух использованных утилит.

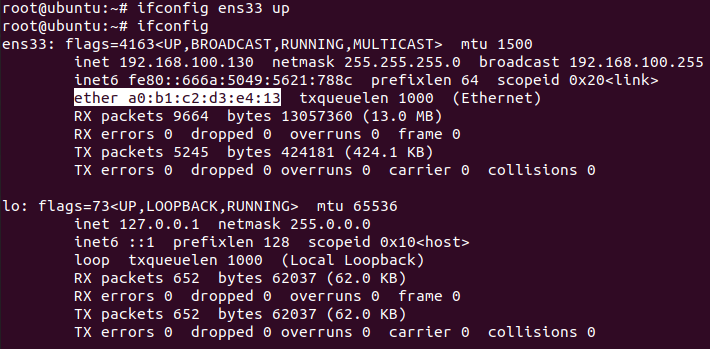


6. Командой ps –ef | more выведите список процессов и убедитесь, что сетевой процесс inetd работает. Иначе его нужно запустить вручную командой inetd. Если исследуемая версия ОС не содержит сервера telnet (по причине его явной уязвимости некоторые версии Linux не предусматривают использования этого протокола), соответствующие пункты задания выполните с защищенной программной оболочкой Secure Shell (SSH).



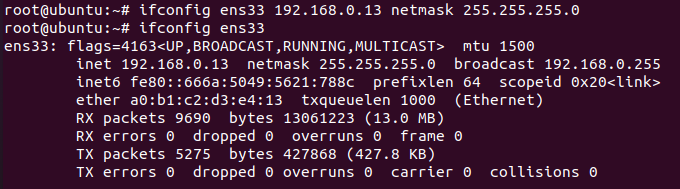
7. Отключите сетевой адаптер командой ifconfig eth0 down (см. справку по сетевым командам). Присвойте сетевому интерфейсу временный MAC-адрес A0:B1:C2:D3:E4:N, где N – двузначный номер вашего компьютера. Подключите адаптер к сети. Убедитесь в том, что его аппаратный адрес изменен.



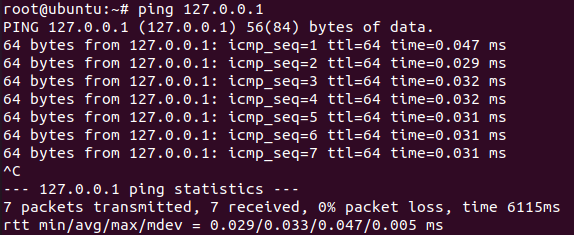


8. Назначьте основному сетевому интерфейсу компьютера временный IP-адрес и маску подсети. Для этого введите команду ifconfig eth0 192.168.0.N netmask 255.255.255.0, где N – номер компьютера. Повторным вводом команды ifconfig eth0 убедитесь в том, что запись введенной информации произведена.

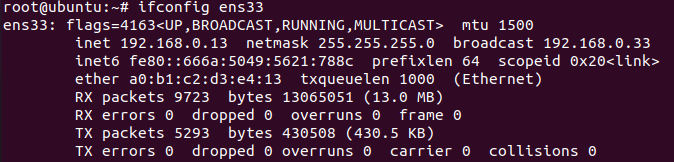
Присвоенные сетевые адреса будут действовать до перезагрузки компьютера.



9. Проверьте работоспособность петли обратной связи, послав на свой же компьютер эхо-запрос ping 127.0.0.1. Убедившись, что отклики поступают, остановите зондирование.

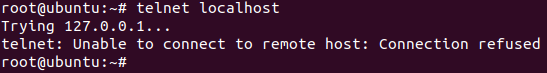


10. Присвойте сетевому адаптеру дополнительный IP-адрес 192.168.0.20+N, где N – номер компьютера. Проверьте прохождение ICMP-пакетов между сетевыми адресами на локальном компьютере.



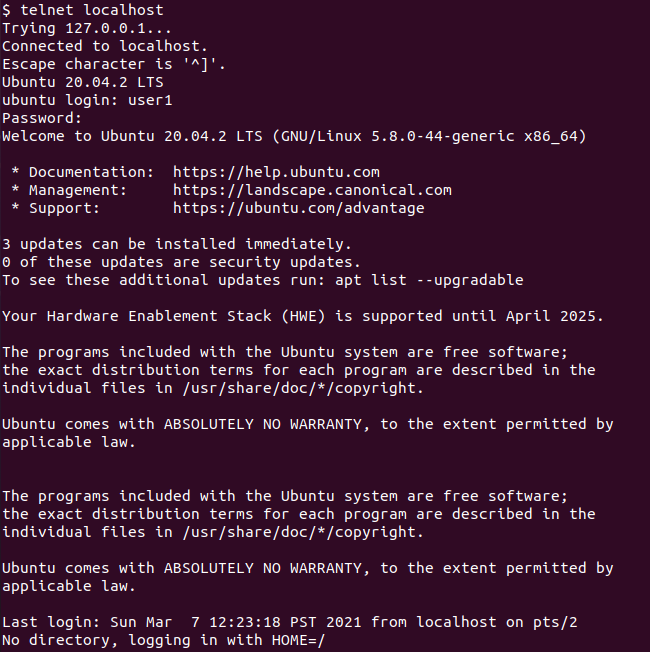
11. Организуйте сеанс telnet на собственном компьютере, используя для этого интерфейс обратной петли или дополнительный IP-адрес (если необходимо, установите из сетевого репозитория пакет telnet в своей операционной системе).

Для этого перейдите в консоль пользователя, наберите команду telnet localhost и после сообщения об успешном соединении введите login и пароль администратора. Почему вам было отказано в доступе?

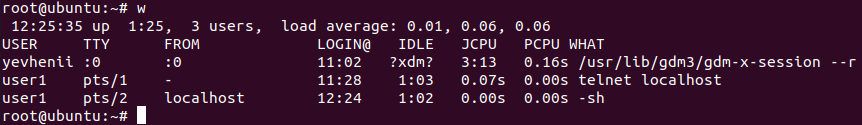


Тому що комп’ютер не очікує з’єднання. Порти закриті.

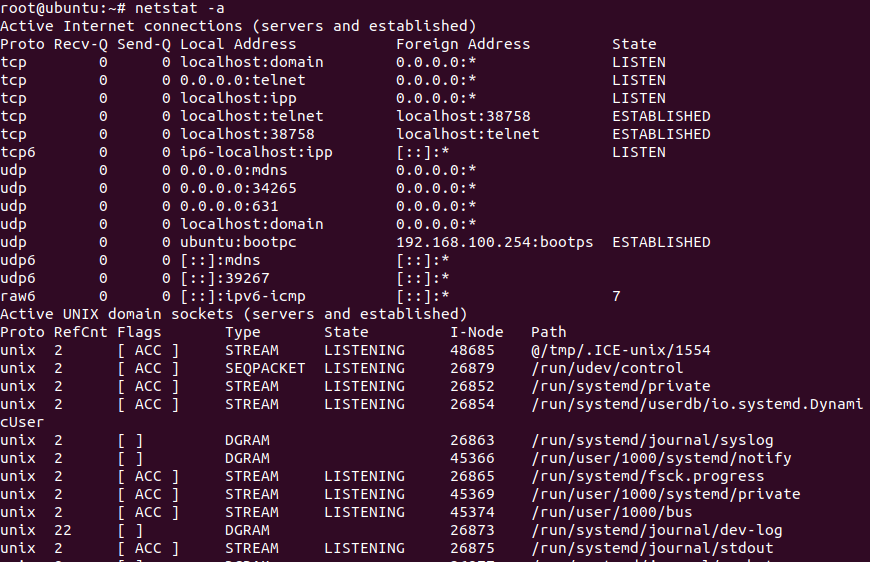
12. Еще раз установите сеанс telnet через петлю обратной связи, используя на этот раз учетную запись обычного пользователя. После установления сеанса просмотрите список каталогов и файлов в нескольких директориях, список процессов и убедитесь, что в «удаленном» режиме доступа вы можете выполнять все команды, которые доступны пользователю, зарегистрированному на удаленном узле.



13. Перейдите в консоль администратора и с помощью команды w или who посмотрите, сколько сейчас пользователей в системе, кто они and wages low и с каких терминалов работают. Обратите внимание на то, как обозначаются локальный и удаленный терминалы.



14. С помощью команды netstat –a проконтролируйте список запущенных сервисов и их состояние.



15. Вернитесь в консоль пользователя и завершите локальный сеанс telnet командой exit. Получите сообщение о закрытии сетевого соединения. Проверьте эту информацию с помощью команды netstat.



16. Попробуйте войти на один из компьютеров сети в сеансе telnet (учетные записи пользователей на всех компьютерах должны быть одинаковы). Что потенциально опасного вы можете сделать на удаленном компьютере?

Я можу створювати, редагувати та видаляти файли.

17. Войдите на произвольный узел по протоколу Secure Shell (команда ssh с указанием IP-адреса хоста, после запроса необходимо ввести пароль администратора). Проверьте свои возможности по манипуляции удаленным компьютером.

18. С помощью команды arp –a посмотрите таблицу соответствия сетевых и аппаратных адресов. Где расположен ARP-кэш и почему он сейчас пуст?

19. С помощью утилиты ping исследуйте локальную сеть, к которой подключен ваш компьютер в диапазоне адресов, идентифицирующих конкретный компьютер в сети, от 1 до 15 (192.168.0.1/15). Объясните, в чем неудобство такого метода сканирования.

20. Проверьте, обновилась ли после сканирования динамическая ARP-таблица. Если она содержит нужную вам информацию о сети, ее можно сохранить в файле командой arp –a > /home/arp1 (через несколько минут информация о сетевых узлах будет изменена, и если тот или иной сетевой узел не проявляет активности, данные о нем в кэше будут утрачены). С помощью команды arp –s <IP-адрес> <MAC-адрес> создайте статическую arp-таблицу. Выясните местоположение этой таблицы.

21. С помощью утилиты nmap исследуйте локальную сеть, к которой подключен ваш компьютер. Что вы можете сказать о полученной информации?

22. Отключите ответы своего сетевого адаптера на ARP-запросы других хостов командой ifconfig eth0 –arp. С помощью команды ifconfig eth0 убедитесь, что настройка выполнена.

23. Выждите несколько минут для сброса ARP-таблиц на компьютерах локальной сети и с одного из компьютеров сети с помощью утилиты ping попробуйте обнаружить отклик своего компьютера. Достаточно ли надежно защищает компьютер от сканирования данная мера? Насколько нарушается при этом возможность работы в сети? Включите arp-отклик командой ifconfig eth0 arp.

24. Отключите сетевой интерфейс на своем компьютере с помощью команды ifconfig eth0 down. Повторите попытку обнаружения своего компьютера с одного из соседних узлов. Можете ли вы сами при этом проявлять какую-либо сетевую активность? Сделайте выводы. Вновь включите сетевой адаптер с помощью команды ifconfig eth0 up.

25. Переведите сетевой адаптер своего компьютера в режим перехвата всех пакетов с помощью команды ifconfig eth0 promisc. С помощью команды ifconfig eth0 убедитесь, что настройка выполнена. При этом сетевой адаптер превращается в устройство подслушивания, но одновременно он становится уязвимым к сетевым атакам на отказ в обслуживании.

26. Ознакомьтесь с синтаксисом команды tcpdump.

27. С помощью утилиты перехватите и прочитайте сетевые пакеты:

- отправленные из одного определенного адреса,

- являющиеся результатом сетевого обмена между двумя хостами сети.

28. Запишите несколько перехваченных пакетов в файл и просмотрите их в шестнадцатеричном коде (приведите для примера скриншот с 4-5 перехваченными пакетами).

Найдите характерные поля и идентификаторы в заголовках канального, сетевого и транспортного уровней. Определите аппаратные и сетевые адреса, номера портов, иные характерные признаки, идентифицирующие сетевые протоколы.

Представьте преподавателю отчет о проделанной работе с выводами по пунктам.

**Висновки**

У цій лабораторній роботі було на практиці