Лабораторна робота №4

Мета роботи: Навчитись налаштовувати мережні інтерфейси в Linux та використовувати діагностичні утиліти (tcpdump, ping, netstat, traceroute, nslookup, dig, iperf, nmap)

Підготовка до виконання роботи

1. Ознайомитись з призначенням та можливостями діагностичних утиліт
   1.1. ping
   1.2. traceroute
   1.3. netstat
   1.4. nslookup
   1.5. dig
   1.6. tcpdump
   1.7. iperf
   1.8. nmap
2. Навчитись підключатися до віддаленого Linux-сервера за допомогою протоколу SSH, копіювати файли з сервера та на сервер за допомогою SFTP/ SCP
3. Навчитись використовувати утиліту wget для завантаження файлів з HTTP / FTP серверів

Порядок виконання роботи

1. Підключитися до сервера (стовпчик А) по SSH
2. Налаштувати мережний інтерфейс ens19 (задати IP-адресу, маску підмережі - стовпчик В)
3. За допомогою утиліти ping перевірити, чи доступні по мережі хости з IP-адресами 172.16.100.195, 172.16.100.196, 172.16.100.190
4. За допомогою утиліти traceroute визначити, через які маршрутизатори проходять пакети до хостів 8.8.8.8, kpi.ua, google.com
5. Перевірити, чи очікує якийсь з процесів на сервері на з’єднання на портах tcp та udp з номерами: 21, 22, 80, 67, 89, 443, 8080
6. Відправити запити до DNS-серверу 10.18.58.195
   6.1.Запитати IP-адресу хоста з ім’ям ws1.okm2020.lab
   6.2.Запитати ім’я хоста з IP-адресою 172.20.10.5
   6.3.Отримати запис типу TXT для домену okm2020.lab
7. Перевірити швидкість передачі даних між вашим сервером та іншим сервером зі стовпчика А (це завдання виконувати в парі з іншим студентом)
8. Знайти в мережі 10.18.58.0/24 всі ввімкнені вузли
9. За допомогою tcpdump перехопити, записати у файл та проаналізувати трафік що передається при
   9.1. перевірці зв’язку за допомогою утиліти ping
   9.2. визначенні маршруту за допомогою traceroute

9.3. завантаженні html-сторінки, файлу з веб-серверу. (Запит можна відправити, наприклад, до 172.16.100.196 та завантажити сторінку index.html, та файл cat.jpg. Або до іншого доступного веб-серверу)

10. Скопіювати файли з трафіком (з попереднього пункту) з віддаленого сервера на локальний комп'ютер, та проаналізувати їх у wireshark. Звернути увагу на:
    - 10.1. IP-адреси до яких відправляються пакети, та номери портів
    - 10.2. DNS -запити
    - 10.3. Послідовність прапорців при встановленні TCP- з'єднання
    - 10.4. Запити та відповіді у протоколах прикладного рівня

	A	B
№	адреса на сервері (інтерфейс ens18)	адреса на сервері на інтерфейсі ens19
1	10.18.58.201	172.16.100.25/24
2	10.18.58.202	172.16.100.24/24
3	10.18.58.203	172.16.100.23/24
4	10.18.58.204	172.16.100.22/24
5	10.18.58.205	172.16.100.21/24
6	10.18.58.206	172.16.100.20/24
7	10.18.58.207	172.16.100.19/24
8	10.18.58.208	172.16.100.18/24
9	10.18.58.209	172.16.100.17/24
10	10.18.58.210	172.16.100.16/24
11	10.18.58.211	172.16.100.15/24
12	10.18.58.212	172.16.100.14/24
13	10.18.58.213	172.16.100.13/24
14	10.18.58.214	172.16.100.12/24
15	10.18.58.215	172.16.100.11/24
16	10.18.58.216	172.16.100.31/24
17	10.18.58.217	172.16.100.32/24
18	10.18.58.218	172.16.100.33/24
19	10.18.58.219	172.16.100.34/24
20	10.18.58.220	172.16.100.35/24
21	10.18.58.221	172.16.100.36/24
22	10.18.58.222	172.16.100.37/24
23	10.18.58.223	172.16.100.38/24
24	10.18.58.224	172.16.100.39/24
25	10.18.58.225	172.16.100.40/24

26	10.18.58.226	172.16.100.41/24
27	10.18.58.227	172.16.100.42/24
28	10.18.58.228	172.16.100.43/24
29	10.18.58.229	172.16.100.44/24
30	10.18.58.230	172.16.100.45/24