Системне програмне забезпечення кіберфізичних систем

Лабораторна робота № 6

НАЗВА: Моніторинг мережних підключень та інтерфейсів в ОС Linux.
МЕТА: Навчитись роботі з командами та системними утилітами моніторингу мережних підключень та інтерфейсів в ОС Linux.

1. Загальні відомості

1.1. Команда **tcpdump** призначена для виводу опису вмістимого пакетів мережного трафіку, які відповідають заданому логічному виразу (boolean expression), для заданого мережного інтерфейсу (network interface). Команду **tcpdump** зручно використовувати для моніторингу та аналізу мережного трафіку з метою відлагодження роботи програм або з метою забезпечення безпеки системи. З опцією -w команда **tcpdump** зберігає отриману інформацію про вмістиме пакетів у вказаному файлі для подальшого аналізу. З опцією -r команда **tcpdump** читає вхідну інформацію не з мережного інтерфейсу, а з вказаного файлу.

Приклади:

1) вивести інформацію про пакети для заданого мережного інтерфейсу (опція -i):
```
$ tcpdump -i eth0
```

2) вивести інформацію про вказану кількість пакетів (опція -c) заданого мережного інтерфейсу:
```
$ tcpdump -c 5 -i eth0
```

3) вивести перелік доступних у системі мережних інтерфейсів:
```
$ tcpdump -D
1.eth0 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth0 (Bluetooth adapter number 0)
5.nflog (Linux netfilter log (NFLOG) interface)
6.nfqueue (Linux netfilter queue (NFQUEUE) interface)
7.usbmon1 (USB bus number 1)
8.usbmon2 (USB bus number 2)
```

4) виводити захоплені пакети у форматі HEX та ASCII:
```
$ tcpdump -XX -i eth0
11:51:18.974360 IP 172.16.25.126.ssh > 172.16.25.125.apwi-rxspooler: Flags [P.], seq
3509235537:3509235733, ack 3652638190, win 18760, length 196
        0x0000:  b8ac 6f2e 57b3 0001 6c99 1468 0800 4510  ..o.W...l..h..E.
        0x0010:  00ec 8783 4000 4006 275d ac10 197e ac10  ....@.@.']...~..
        0x0020:  197d 0016 1129 d12a af51 d9b6 d5ee 5018  .}...).*.Q....P.
        0x0030:  4948 8bfa 0000 0e12 ea4d 22d1 67c0 f123  IH.......M".g..#
        0x0040:  9013 8f68 aa70 29f3 2efc c512 5660 4fe8  ...h.p).....V`O.
        0x0050:  590a d631 f939 dd06 e36a 69ed cac2 95b6  Y..1.9...ji.....
.   .   .
```

5) зберігати захоплені пакети у вказаний файл (опція -w):
```
$ tcpdump -w 0001.pcap -i eth0
```

6) прочитати захоплені пакети з вказаного файлу (опція -r):

$ tcpdump -r 0001.pcap

7) захоплювати лише TCP-пакети:
$ tcpdump -i eth0 tcp

8) захоплювати пакети зі вказаного мережного порту:
$ tcpdump -i eth0 port 22

9) захоплювати пакети зі вказаною ip-адресою відправника:
$ tcpdump -i eth0 src 192.168.0.2

10) захоплювати пакети зі вказаною ip-адресою отримувача:
$ tcpdump -i eth0 dst 50.116.66.139

1.2. Системна утиліта **ss** (**s**ocket **s**tatistics) призначена для отримання інформації про мережні сокети. Утиліту **ss** зручно використовувати для моніторингу мережних під'єднань. За допомогою **ss** можна 1) отримати детальну інформацію про те, як даний комп'ютер взаємодіє з іншими комп'ютерами, мережами та службами; 2) дізнатись подробиці про роботу мережних з'єднань, статистику використання мережних протоколів та сокетів. Використання утиліти **ss** полегшує вирішення проблем з мережними підключеннями.

Приклади:

1) вивести список всіх мережних підключень (сокетів):
$ ss

2) вивести список всіх TCP-з'єднань:
$ ss -t

3) вивести ідентифікатори процесів, яким «належать» мережні сокети:
$ ss -p

4) вивести мережні з'єднання для заданої ip-адреси:
$ ss dst 192.168.1.139

5) вивести мережні з'єднання для заданого номеру мережного порту:
$ ss -at '(dport = :22 or sport = :22)'

6) вивести загальну інформацію про мережні з'єднання (загальна кількість встановлених з'єднань, кількість сокетів різних типів, використання протоколів IPv4/IPv6 та ін.):
$ ss -s

```
Total: 940 (kernel 0)
TCP:   9 (estab 2, closed 1, orphaned 0, synrecv 0, timewait 1/0), ports 0

Transport Total     IP        IPv6
*         0         -         -
RAW       1         0         1
UDP       17        13        4
TCP       8         5         3
INET      26        18        8
FRAG      0         0         0
```

1.3. Системна утиліта **iftop** за аналогією до команди top виводить динамічний список найактивніших мережних з’єднань для заданого мережного інтерфейсу. За допомогою опції -i можна вказати назву мережного інтерфейсу, для якого буде виводитись список з’єднань. З’єднання у списку відсортовані за спаданням об’єму мережного трафіку (current bandwidth usage). За допомогою опції -P можна включити додаткове відображення номеру порту. Так само як і команда top, утиліта **iftop** є інтерактивною. Приклади команд: s - включити/виключити відображення адреси відправника, d - включити/виключити відображення адреси отримувача, p - включити/виключити режим паузи.

2. Послідовність виконання роботи

2.1. Ознайомитись з відомостями про моніторинг мережних підключень та інтерфейсів в ОС Linux.
2.2. Дослідити роботу команди tcpdump. За допомогою цієї команди:
1) вивести інформацію про пакети для заданого мережного інтерфейсу;
2) вивести інформацію для заданої кількості пакетів заданого мережного інтерфейсу;
3) вивести перелік доступних у системі мережних інтерфейсів;
4) вивести захоплені пакети у форматі HEX та ASCII;
5) зберігти захоплені пакети у вказаний файл;
6) прочитати захоплені пакети з вказаного файлу;
7) захоплювати лише TCP-пакети;
8) захоплювати пакети зі вказаного мережного порту;
9) захоплювати пакети зі вказаною ip-адресою відправника;
10) захоплювати пакети зі вказаною ip-адресою отримувача.
2.3. Дослідити роботу системної утиліти ss. Вивести за її допомогою
1) список всіх мережних підключень (сокетів);
2) список всіх TCP-з’єднань;
3) ідентифікатори процесів, яким «належать» сокети;
4) мережні з’єднання для заданої ip-адреси;
5) мережні з’єднання для заданого номеру мережного порту;
6) загальну інформацію про мережні з’єднання.
2.4. Дослідити роботу системної утиліти iftop.
2.5. Скласти та захистити звіт з лабораторної роботи.

3. Зміст звіту

3.1. Результати виконання завдань по дослідженню роботи команди tcpdump.
3.1. Результати виконання завдань по дослідженню роботи системної утиліти ss.
3.2. Результати дослідження роботи системної утиліти iftop.

4. Контрольні питання

4.1. Призначення та використання команди tcpdump.
4.1. Призначення та використання системної утиліти ss.
4.2. Призначення та використання системної утиліти iftop.

5. Джерела

1. Daniel P. Bovet, Marco Cesati, Understanding the Linux Kernel, 3rd edition, O'Reilly Media, 2005. - 944 p.

2. Robert Love, Linux Kernel Development, 3rd edition, Addison-Wesley Professional, 2010. - 440 p.

3. The Linux Kernel documentation, www.kernel.org/doc/html/latest/