XVII. Thực hành giám sát mạng

Các bước trong bài thực hành như sau:

1) Cài đặt các công cụ clients trên 2 servers

2) Tạo file log chứa thông tin lưu lượng mạng

1. **Cài đặt các công cụ trên 2 máy Linux server làm máy chủ và máy client**

- Chúng ta phải cài đặt hai công cụ mà nhóm phát triển phần mềm sẽ sử dụng để tạo và theo dõi lưu lượng mạng.
- Sử dụng lệnh YUM để cài đặt trên máy chủ server1:

```
[root@server1]# yum install iptraf-ng nc
```

- Cài đặt 2 công cụ này trên máy chủ khác là server2:

```
[root@server2]# yum install iptraf-ng nc
```

- **Tạo file nhật ký log chứa thông tin lưu lượng mạng:**

- Trên máy chủ server 1, hãy chạy iptraf-ng và vào phần Cấu hình... Trong menu, đây là menu chúng ta điều khiển bằng bàn phím. Vào mục "IP traffic monitor".
- Trong menu tiếp theo, chọn eth0 Đặt đường dẫn file nhật ký log thành: /root/traffic_log.txt.
- Sau đó nhấn Enter vào màn hình lưu lượng IP. . và quá trình ghi nhật ký log file sẽ bắt đầu.

2. **Lắng nghe thông tin lưu lượng mạng giữa 2 máy servers**

- Hãy mở terminal thứ hai vào server1 để thực hiện việc bắt đầu để server 1 nghe netcat trên cổng 2525 với lệnh sau:

```
[root@server1]# nc -l 2525
```

- Gửi một số lưu lượng truy cập mạng từ server 2 vào server1
- Quay lại terminal của server2 mà chúng ta đã mở, gửi lưu lượng netcat đến server1 bằng lệnh nc (trong đó x.x.x.x là IP nội bộ của server1):

```
[root@server2]# nc x.x.x.x 2525
```

- Nó sẽ cho phép chúng ta nhập 1 số thông điệp, và chúng ta có thể nhập một số thông điệp tại dấu nhắc và nhấn Enter.
- Khi chúng ta thực hiện lệnh trên, nó sẽ hiển thị lại trong cửa sổ mà chúng ta đang nghe trên server1.

3. **Một loạt các thông điệp được gửi từ server2 sẽ giống như ở dưới:**

[root@server2]# nc x.x.x.x 2525

test

test

test

This is a test

- Trên server1, các thông điệp từ server2 gửi đến sẽ hiển thị lên Terminal như dưới:

[root@server1]# nc -l 2525

test

test

test

This is a test

- Như vậy là đủ thông tin lưu lượng truy cập được gửi từ server2 đến server1. Trên server2, nhấn Ctrl + C để tắt lệnh nc mà chúng ta đang chạy và quay lại terminal trên server 1 mà chúng ta đang chạy công cụ iptraf-ng. Nhấn x để dừng theo dõi và thoát ra, sau đó chọn Exit Thoát khỏi menu chính.Kiểm tra File log chứa thông tin lưu lượng mạng
- Trên server1, nếu chúng ta chạy ls ls /var/log/iptraf-ng/, chúng ta sẽ thấy iptraffic.txt được liệt kê . Đọc nó để xem nó có nắm bắt được những gì chúng ta cần không:

[root@server1]# less /var/log/iptraf-ng/iptraffic.txt

- Chúng ta sẽ thấy nội dung của file này hiển thị lưu lượng truy cập từ server2 đến server1 trên cổng 2525.