**Tìm hiểu cách dùng Tcpdump cơ bản**

**1. Giới thiệu**

tcpdump là phần mềm bắt gói tin trong mạng làm việc trên hầu hết các phiên bản hệ điều hành Linux. tcpdump cho phép chúng ta bắt và lưu lại các gói tin bắt được, để chúng ta có thể sử dụng phân tích.

**Cài đặt để sử dụng**

Đối với Ubuntu, ta dùng lệnh

# sudo apt-get install tcpdump -y

CentOS

# yum install tcpdump -y

**Một số lệnh, option cơ bản thường dùng và ví dụ**

Các tùy chọn thường sử dụng trong tcpdump:

-X : Hiển thị nội dung của gói theo định dạng ASCII và HEX

-XX : Tương tự -X, hiển thị giao diện ethernet

-D : Liệt kê các giao diện mạng có sẵn

-l : Đầu ra có thể đọc được dòng (để xem khi bạn lưu hoặc gửi đến các lệnh khác)

-t : Cung cấp đầu ra dấu thời gian có thể đọc được của con người

-q : Ít dài dòng hơn với đầu ra

-tttt : Cung cấp đầu ra dấu thời gian tối đa có thể đọc được của con người

-i : Bắt lưu lượng của một giao diện cụ thể

-vv : Đầu ra cụ thể và chi tiết hơn (nhiều v hơn cho đầu ra nhiều hơn)

-s : Xác định snaplength(kích thước) của gói tin theo byte. Sử dụng -s0 để có được mọi thứ. Nếu không set size packet dump thành unlimit, thì khi tcpdump ra nó bị phân mảnh

-c : Chỉ nhận được x số gói và sau đó dừng lại

-S : In số thứ tự tuyệt đối

-e : Nhận tiêu đề ethernet

-q : Hiển thị ít thông tin giao thức

-E : Giải mã lưu lượng IPSEC bằng cách cung cấp khóa mã hóa

Để bắt các gói tin có địa chỉ IP dùng option -n. Nếu không dùng tùy chọn này chỉ bắt được các gói tin chứa các địa chỉ DNS thay vì địa chỉ IP.

Ví dụ: # tcpdump -n -i eth0

Bắt gói tin từ một giao diện ethernet cụ thể dùng option -i.

Ví dụ: # tcpdump -n -i eth1

Chỉ bắt số lượng N gói tin dùng option -c

Ví dụ: # tcpdump -c 10 -i eth0

Hiển thị các gói tin đã bắt trong ASCII

Ví dụ: # tcpdump -A -n -i eth0

Một số người dùng có thể muốn phân tích các gói theo giá trị hex. tcpdump cung cấp một cách để in các gói ở cả định dạng ASCII và HEX.

Ví dụ: # tcpdump -XX -n -i eth0

Bắt các gói tin và lưu vào 1 file .pcap

Ví dụ: # tcpdump -w vidu.pcap -i eth0

Đọc các gói từ một file .pcap đã lưu

Ví dụ: # tcpdump -r vidu.pcap

Chỉ nhận các gói của một loại giao thức cụ thể Chúng ta có thể nhận các gói dựa trên loại giao thức. Có thể chỉ định một trong các giao thức này: fddi, tr, wlan, ip, ip6, arp, rarp, decnet, tcp và udp.

Ví dụ để bắt các gói arp qua giao diện eth0 # tcpdump -n -i eth0 arp

Bắt các gói trên một port cụ thể

Ví dụ bắt các gói tin trên port 22 (SSH) # tcpdump port 22 -i eth0

Một số giao thức được hỗ trợ capture mà không cần phần lệnh lọc như: tcp, udp, icmp, ip, ip6, arp, rarp, atalk, aarp, decnet, iso, stp, ipx, netbeui

Ví dụ: # tcpdump -n -i eth0 not arp and not rarp

**Một số tùy chọn bộ lọc sử dụng với tcpdump:**

Sử dụng trong tùy chọn [expression] trong câu lệnh tcpdump.

and, or, not : sử dụng kết hợp các bộ lọc.

dst host host : lọc các gói tin có địa chỉ IP hoặc tên host đích của gói tin là host

src host host: tương tự như trên với địa chỉ nguồn của gói tin.

host host\_addr : lọc nếu trong gói tin có địa chỉ nguồn hoặc đích bằng với host\_addr

ether dst host ehost : lọc gói tin nếu MAC đích của gói tin ethernet có giá trị là ehost

ether src host ehost: tương tự với giá trị là MAC nguồn.

ether host ehost :lọc gói tin nếu gói tin ethernet có MAC đích hoặc MAC nguồn là ehost

dst port port : lọc gói tin nếu gói tin bắt được có port đích bằng với port

src port port và port port cũng tương tự như trên.

dst portrange port1-port2 lọc gói tin nếu gói tin có địa chỉ port dích nằm trong khoảng từ port1 tới \*port2

src portrange port1-port2 và portrange port1-port2 ý nghĩa tương tự.

less length : lọc nếu gói tin có kích thước nhỏ hơn hoặc bằng length (tính bằng byte)

greater length: lọc nếu gói tin có kích thước lớn hơn hoặc bằng length

ip proto protocol: lọc các gói tin ipv4 có giao thức là protocol. Ví dụ: tcp, udp, icmp, arp

ether broadcast: lọc các gói tin gửi broadcast layer 2.

vlan vlan\_id lọc các gói tin thuộc vlan\_id.

Tham khảo: <https://blogd.net/linux/vi-du-ve-su-dung-lenh-tcpdump/>

<https://github.com/hocchudong/thuctap012017/blob/master/TamNT/T%C3%ACm%20hi%E1%BB%83u%20c%C3%B4ng%20c%E1%BB%A5%20tcpdump.md#:~:text=Gi%E1%BB%9Bi%20thi%E1%BB%87u%20tcpdump,t%C3%ADnh%20m%C3%A0%20n%C3%B3%20tham%20gia.&text=V%E1%BB%9Bi%20option%20%2Dw%2C%20ng%C6%B0%E1%BB%9Di%20d%C3%B9ng,g%C3%B3i%20tin%20d%C6%B0%E1%BB%9Bi%20d%E1%BA%A1ng%20file%20>.