**TCP/IP Hacking**

Mô hình DoD – Department of Defense:

* Tầng ứng dụng(Process/Application Layer)
* Tầng giao vận(Host-to-Host Layer)
* Tầng liên mạng(Internet Layer)
* Tầng giao diện mạng (Network Access Layer)
* Tầng giao diện mạng: có trách nhiệm truyền/ nhận dữ liệu trong cùng 1 mạng. Các phần cứng vật lí như là card mạng(card Ethernet), cáp mạng

Một số giao thức tiêu biểu:

- ATM(Asynchronous Transfer Mode)

- Ethernet

- Token Ring

- FDDI(Fiber Distributed Data Interface)

- Frame Relay

* Tầng liên mạng: có chức năng đánh địa chỉ, đóng gói dữ liệu, định tuyến dữ liệu

Các giao thức của tầng bao gồm:

- IP(Internet Protocal): giao thức được sử dụng rộng rãi trong mọi hệ thống mạng(phạm vi toàn thế giới)

- ICMP(Internet Control Message Protocol): cung cấp chức năng thông báo lỗi trong trường hợp dữ liệu truyền bị hỏng

- IGMP(Internet Group Message Protocol): chức năng điều khiển, truyền dẫn đa hướng, multicasting(là khi 1 nhóm thiết bị đều nhận được các thông điệp hoặc packets giống nhau). Ví dụ: 1 số thiết bị chia sẻ 1 địa chỉ IP để tất cả chúng có thể nhận cùng 1 dữ liệu

* Tầng giao vận: chức năng chính là xử lí vấn đề giao tiếp giữa các má chủ trong cùng 1 mạng hoặc khác mạng kết nối với nhau thông qua bộ định tuyến. Tại đây dữ liệu được phân đoạn sẽ không bằng nhau nhưng nhỏ hơn 64KB

Gồm 2 giao thức cốt lõi: TCP và UDP

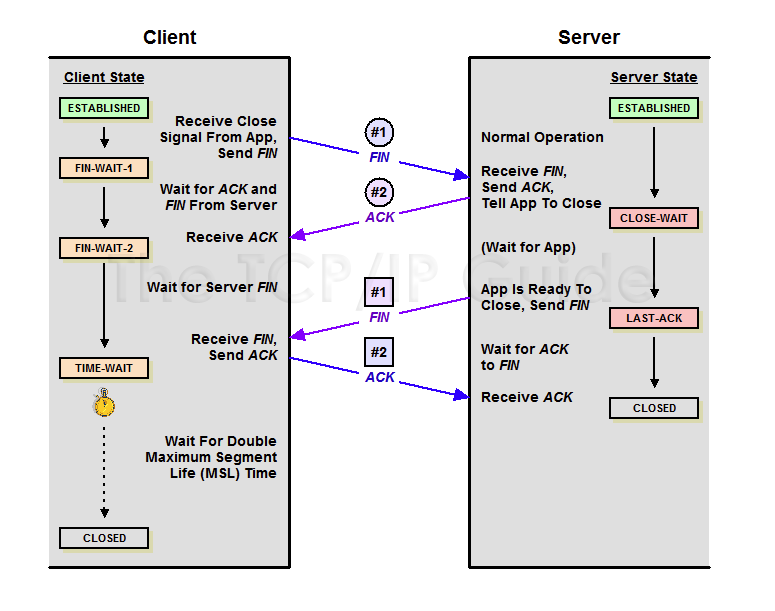
* Tầng ứng dụng: Đảm bảo vai trò giao tiếp dữ liệu giữa 2 máy khác nhau thông qua các dịch vụ mạng và 1 số giao thức trao đổi dữ liệu:SMTP,SSH,FTP,… Dữ liệu ở đây được định dạng theo kiểu Byte nối Byte
* Quy trình hoạt động các gói tin(packet)

Lớp Application: lớp gần nhất với tương tác người dùng. Dữ liệu ở đây sẽ được đóng gói, định dạng theo giao thức sử dụng và mã hóa nếu yêu cầu. -> Lớp Transport: Tại đây dữ liệu sẽ được phân đoạn. Các phần phân đoạn sẽ được đóng gói với một header, header được thêm vào để xác định thông tin như port nguồn, port đích, thông tin kiểm lỗi, đánh dấu thứ tự,… tất cả để máy đích khi nhận được sẽ ghép lại thành 1 khối dữ liệu hoàn chỉnh. Được gọi là segment. -> Lớp NetWork: tại đây các segment được gắn thêm một header gọi là IP Header bao gồm 2 thông tin chính là Source IP và Destination IP. Các gói bây giờ được gọi là Packet -> Lớp DataLink: để một gói tin có thể gửi tới đích cần thêm 1 loại địa chỉ nữa đó là địa chỉ MAC hay địa chỉ vật lí. Độc nhất trên mọi thiết bị. Tầng này sẽ ghép frame header và frame trailer lần lượt vào đầu và cuối packet. Các packet bây giờ được gọi là frame.

Các trạng thái TCP:

Client TCP States:

The client process sends an *open call* to its TCP for a connection request to a specific socket. This called an *open active*. In this case TCP sends SYN to the server and client TCP moves to SYN-Sent state. At this time Server is in LISTEN state until it received SYN from Client it will send SYN + ACK back to client and move to SYN-RCVD state. After client receive SYN + ACK from server it will send ACK back to server and move to ESTABLISHED state, server also placed in this state when it received ACK from client. In this state data can transfer in both directions. Now if the client process has no more data to send, it will then perform an *active close call*. When this happens, the client will send FIN to the server and goes to FIN-WAIT-1 state. And then server have received FIN from client move to CLOSE-WAIT state after send ASC to client. So in client now receive ACK of the sent FIN(from FIN-WATE-1 state) and move to FIN-WAIT-2. It will remain this state till it does not receive FIN from server. At some stage the server application will initiate the close call to TCP. When it does server TCP will send FIN and move to LAST-ACK state. It will remain LAST-ACK state until received ACK for it and will move to CLOSED state once ACK received. Now when client received FIN from server, it sends ACK back and move to TIME\_WAIT state, it then sets the timer to twice the maximun segment length(MSL). The common value for MSL is 30 to 1 min.



**Server and Linux**

Phân biệt Server – Desktop:

* NIC – Network Interface Card: Máy tính để bàn hoặc máy tính xách tay chỉ có một NIC. NIC(card giao diện mạng) là 1 phần rất quan trọng của bất kì thiết bị nào và yêu cầu phải được kết nối mạng. Card này giúp thiết lập liên kết với thiết bị đó và mạng.

Trong các máy chủ số lượng NIC sẽ từ 2 trở lên. Vì 1 server thường phục vụ cho mục đích đặc biệt và phải có sẵn/trực tuyến 24/7. Đôi khi số lượng NIC có thể lên tới 8 – 16 tùy theo yêu cầu.

* CPU – Central Processing Unit/ Bộ xử lí trung tâm: CPU được ví như bộ não của hệ thống. Sức mạnh CPU càng cao thì các tác vụ sẽ được tiến hành càng nhanh. Có sự khác biệt lớn trong bộ vi xử lí cấp máy tính đề bàn/xách tay và máy chủ. Tất cả chúng đều có nhiều loại socket, khả năng xử lí, model và thế hệ. Các bộ xử lí cấp máy chủ đắt tiền hơn các bộ vi xử lí thông thường dành cho máy tính để bàn.
* RAM(Random Access Memory): thông thường RAM 4GB đến 8GB là đủ cho máy tính để bàn/xách tay dùng. Tuy nhiên đối với máy chủ, yêu cầu sẽ cao hơn rất nhiều, con số lên tới 128GB, 1.5TB, 4TB.
* Bộ nhớ: Đối với những máy thông thường 100GB hoặc 300GB là đủ dùng tuy nhiên ới máy chủ đòi hỏi không gian bộ nhớ rất lớn. Khoảng 500GB đến 2-3TB. Chi phí cho dung lượng dự trữ rất tốn kém và nó phụ thuộc vào yêu cầu của máy chủ.

**RAID – Redundant Array ò Inexpensive Disks hoặc Redundant Arrays of independent Disks**

Là 1 kỹ thuật ảo hóa cho phép gom nhiều ổ đĩa cứng vật lí thành 1 hệ thống ổ đĩa logic nhằm mục đích gia trăng tốc độ truy xuất dữ liệu hoặc giảm nguy cơ mất, hỏng dữ liệu do lỗi đĩa phần cứng gây ra hoặc đôi khi kết hợp cả 2 mục đích trên.

Cách thức hoạt động của RAID là sao chép dữ liệu lên 2 hoặc nhiều ổ cứng vật lí được liên kết với nhau bằng 1 RAID Controller.

Có nhiều cách cài đặt RAID khác nhau, mỗi liệu RAID lại phục vụ 1 mục tiêu khác nhau dựa trên những nhu cầu cụ thể để giải quyết các yêu cầu.

Các loại RAID phổ biến:

* RAID 1: khả năng đảm bảo an toàn dữ liệu
* RAID 5: hiệu quả năng suất được nâng cao, bảo mật dữ liệu cao
* RAID 6: sự phát triển hơn RAID 5
* RAID 10: lưu trữ nhanh và an toàn, nâng cao hiệu suất, đảm bảo dữ liệu không mất khi 1 trong 4 ổ bị hỏng

OS dành cho server:

Windows:

Ưu điểm:

* Giao diện than thiện, dễ sử dụng
* Cập nhập vá lỗi thường xuyên
* Sử dụng rộng rãi dễ dàng đồng bộ với Client

Nhược điểm:

* Có tính chi phí(bản quyền)
* Mã nguồn rất hạn chế không có nhiều tùy chỉnh
* Mức độ phổ biến cao nên là 1 mục tiêu của Hacker

Linux:

Ưu điểm:

* Đa số phần mềm, ứng dụng miễn phí
* Tối ưu phần cứng, tăng hiệu năng xử lí máy chủ
* Phổ biến các thiết bị thông minh hiện nay(android, WebOS,..)

Nhược điểm:

* Giao diện chưa thân thiện, phần lớn sử dụng bằng câu lệnh
* Số lượng phần mềm hạn chế, không có nhiều lựa chọn
* Ít được hỗ trợ driver phần cứng mới

MAC OS X Server

Ưu điểm:

* Độ ổn định cao, sử dụng mượt
* Tính bảo mật cao thường xuyên được cập nhập
* Tối ưu hóa sử dụng, tương thích cao với các thiết bị của Apple

Nhược điểm:

* Gía thành cao so với các OS khác
* Chỉ tương thích phần cứng của Apple, hạn chế hỗ trợ với các phần cứng vào phần mềm thứ ba
* Sự lựa chọn phần mềm tương đối ít
* Cộng đồng người dùng tại Việt Nam không lớn

Ngoài ra có các OS khác như: CentOs, Red hat enterprise linux, Ubuntu, Debian, Fedora, FreeBSD, HP-UX, Solaris

**Hệ thống tập tin Linux(FileSystem)**

* *Cấu trúc thư mục:*

Bạn sẽ không tìm thấy bất kỳ thư mục Windows, tệp chương trình hoặc người dùng nào nếu duyệt qua hệ thống tệp trên máy tính linux của mình

Cấu trúc thư mục Linux không chỉ sử dụng khác nhau cho các thư mục, nó còn sử dụng bố cục hoàn toàn khác.

Ví dụ trên windows 1 ứng dụng có thể lưu trữ tất cả các tệp của nó trong C:\ProgarmFiles\NameApp nhưng trên Linux tệp của nó sẽ được phân chia giữa nhiều vị trí nhị phân của nó trong /usr/bin. Các thư viện của nó trong /usr/lib và các tệp cấu hình của nó trong /etc/

* Độ nhạy trường hợp:

Trên Linux, hệ thống tệp phân biệt chữ hoa chữ thường trong cùng 1 thư mục. Tuy nhiên ở windows thì không.

Windows sử dụng gạch chéo ngược so với dấu gạch chéo “\” còn trên Linux sẽ là “/”, điều này cũng đúng trong các URL trình duyệt Web của bạn.

* *Không có ký tự ổ đĩa:*

Trên Linux, mọi thứ đều nằm dưới / - thư mục gốc. Không có tệp nào trên thư mục gốc nhưng với windows thì khác, cho dù bạn có nhiều ổ đĩa cứng, nhiều phân vùng trên cùng 1 ổ đĩa cứng hoặc các thiết bị di động được kết nối, mỗi hệ thống tệp đều có sẵn dưới tên ổ đĩa riêng của nó.

* *Mọi thứ đều là 1 tập tin:*

Giống như mọi hệ thống tệp được gắn kết là 1 thư mục bên dưới /(thư mục gốc), mọi thứ trên Linux là 1 tệp.

* *Bạn có thể xóa hoặc sửa đổi các tệp đang mở:*

Trên Linux bạn thường có thể xóa hoặc sửa đổi tệp video khi nó đang phát, còn trên Windows sẽ không được

**Trình soạn thảo VIM – Thực hành**