HackerVN Hack FAQ

Lời nói đầu: Thể theo yêu cầu của mọi người, ban điều hành HackerVn đã cho ra đời bản FAQ này dành cho những bạn mới làm quen với nghệ thuật Hacking và Internet. Bạn có thể tự tìm tòi những điều căn bản mà bất cứ Hacker nào cũng phải "master". Hy vọng những khái niệm trong bài viết này sẽ giải đáp được nhiều thắc mắc của một số bạn. Nếu bạn cảm thấy những kiến thức dưới đây không đúng hoặc thiếu chính xác bạn có thể gửi thư góp ý .

Bản FAQ này dựa trên cơ sở đóng góp, góp ý của các thành viên trên HackerVN community, vậy nếu bạn có câu hỏi hay giải đáp muốn chúng tôi thêm vào bản FAQ này thì xin liên hệ với địa chỉ e-mail ở trên hoặc có thể gửi lên trên forum. Để trang trở nên thật sự hữu ích và để giúp HackerVN tiến lên phía trước chúng tôi thiết tha sự giúp đỡ và đóng góp của bạn. "Một cây làm chẳng nên non, ba cây chụm lại nên hòn núi cao".

Internet

Địa chỉ IP (IP Address)

(By Conan_Dole and BlackArt)

Trên mạng Internet nó sẽ xác định chính bạn. Khi kết nối vào mạng thì IP của bạn là duy nhất trên thế giới. Tuy nhiên số này chưa hẳn là cố định. Nếu bạn vào mạng qua một ISP thì số IP của bạn sẽ thay đổi ở các lần bạn kết nối. Một người biết IP của bạn thì có thể lần ra vị trí của bạn. Nghĩa là khi có IP thì biết được địa chỉ của ISP rồi biết được thông tin của bạn. Trên thực tế, IP cho biết về máy tính được sử dụng để vào mạng chứ không cho biết thông tin về người sử dụng, trừ khi IP của bạn là cố định hoặc sử dụng account của riêng bạn.
Sự khác nhau giữa logic (hostname) và một địa chỉ IP:
Đơn giản chỉ bởi vì việc gọi tên, ví dụ www.yourname.com sẽ dễ hơn nhiều đối với việc phải gọi 202.32.156.14. Tuy vậy, có một sự khác biệt quan trọng giữa 2 điều này. IP là số để xác định thiết bị (device) còn hostname là một mối liên kết giữa 1 từ khoá và một số IP. Một địa chỉ IP có thể có nhiều hostname khác nhau nhưng một hostname thì chỉ có một IP liên kết với nó.
Địa chỉ IP được chia thành 4 số giới hạn từ 0 - 255. Mỗi số được lưu bởi 1 byte -> !P có kicks thước là 4byte, được chia thành các lớp địa chỉ. Có 3 lớp là A, B, và C. Nếu ở lớp A, ta sẽ có thể có 16 triệu địa chỉ, ở lớp B có 65536 địa chỉ. Ví dụ: Ở lớp B với 132.25,chúng ta có tất cả các địa chỉ từ 132.25.0.0 đến 132.25.255.255. Phần lớn các địa chỉ ở lớp A llà sở hữu của các công ty hay của tổ chức. Một ISP thường sở hữu một vài địa chỉ lớp B hoặc C. Ví dụ: Nếu địa chỉ IP của bạn là 132.25.23.24 thì bạn có thể xác định ISP của bạn là ai. (có IP là 132.25.x.)

IP thể hiện điều gì:

Trên mạng Internet nó sẽ xác định chính bạn. Khi kết nối vào mạng thì IP của bạn là duy nhất trên thế giới. Tuy nhiên số này chưa hẳn là cố định. Nếu bạn vào mạng qua

một ISP thì số IP của bạn sẽ thay đổi ở các lần bạn kết nối. Một người biết IP của bạn thì có thể lần ra vị trí của bạn. Nghĩa là khi có IP thì biết được địa chỉ của ISP rồi biết được thông tin của bạn. Trên thực tế, IP cho biết về máy tính được sử dụng để vào mạng chứ không cho biết thông tin về người sử dụng, trừ khi IP của bạn là cố định hoặc sử dụng account của riêng bạn.

Sự khác nhau giữa logic (hostname) và một địa chỉ IP:

Đơn giản chỉ bởi vì việc gọi tên, ví dụ http://www.yourname.com/ sẽ dễ hơn nhiều đối với việc phải gọi 202.32.156.14. Tuy vậy, có một sự khác biệt quan trọng giữa 2 điều này. IP là số để xác định thiết bị (device) còn hostname là một mối liên kết giữa 1 từ khoá và một số IP. Một địa chỉ IP có thể có nhiều hostname khác nhau nhưng một hostname thì chỉ có một IP liên kết với nó.

IP spoofing là gì:

Một số IP có mục đích để xác định một thiết bị duy nhất trên thế giới. Vì vậy trên mạng một máy chủ có thể cho phép một thiết bị khác trao đổi dữ liệu qua lại mà không cần kiểm tra máy chủ.
Tuy nhiên có thể thay đổi IP của bạn, nghĩa là bạn có thể gởi một thông tin giả đến một máy khác mà máy đó sẽ tin rằng thông tin nhận được xuất phát từ một máy nào đó (tất nhiên là không phải máy của bạn). Bạn có thể vượt qua máy chủ mà không cần phải có quyền điều khiển máy chủ đó. Điều trở ngại là ở chỗ những thông tin phản hồi từ máy chủ sẽ được gởi đến thiết bị có IP mà chúng ta đã giả mạo. Vì vậy có thể bạn sẽ không có được sự phản hồi những thông tin mà mình mong muốn. Có lẽ điều duy nhất mà spoof IP có hiệu quả là khi bạn cần vượt qua firewall, trộm account và cần dấu thông tin cá nhân!

Cổng ảo là gì? (Virtual Port)

Cổng ảo là 1 số tự nhiên được gói ở trong TCP(Tranmission Control Protocol) và UDP(User Diagram Protocol) header (hiện có lẽ bạn còn xa lạ với 2 từ này, chúng tôi sẽ đề cập sau). Như mọi nguời đã biết, Windows có thể chạy nhiều chương trình 1 lúc, mỗi chương trình này có 1 cổng riêng dùng để truyền và nhận dữ liệu. Ví dụ 1 máy có địa chỉ IP là 127.0.0.1 chạy WebServer, FTP_Server, POP3 server, etc, những dịch vụ này đều đuọc chạy trên 1 IP address là 127.0.0.1, khi một gói tin đuọc gửi đến làm thế nào máy tính của chúng ta phân biệt được gói tin này đi vào dịch vụ nào WebServer hay FTP server hay SMTP? Chính vì thế Port xuất hiện. Mỗi dịch vụ có 1 số port mặc định, ví dụ FTP có port mặc định là 21, web service có port mặc định là 80, POP3 là 110, SMTP là 25 vân vân.... Người quản trị mạng có thể thay đổi số port mặc định này, nếu bạn ko biết số port trên một máy chủ, bạn ko thể kết nối vào dịch vụ đó được. Chắc bạn đã từng nghe nói đến PORT MAPPING nhưng có lẽ chưa biết nó là gì và chức năng thế nào. Port mapping thực ra đơn giản chỉ là quá trình chuyển đổi số port mặc định của một dịch vụ nào đó đến 1 số khác. Ví dụ Port mặc định của WebServer là 80, nhưng thỉnh thoảng có lẽ bạn vẫn thấy http://www.xxx.com:8080/ , 8080 ở đây chính là số port của host xxx nhưng đã được nguời quản trị của host này "map" từ 80 thành 8080.

RFC là gì?

RFC là viết tắt của Request For Comment, là tập hợp những tài liệu về kiến nghị, đề xuất và những lời bình luận liên quan trực tiếp hoặc gián tiếp đến công nghệ, nghi thức mạng INTERNET. Các tài liệu RFC được chỉnh sửa, thay đổi đến khi tất cả các kỹ sư thành viên của IETF(Internet Engineering Task Force) đồng ý và duyệt, sau đó những tài liệu này được xuất bản và được công nhận là 1 chuẩn, nghi thức cho Internet. Tài liệu RFC nổi tiếng và làm tạo được tiếng vang lớn nhất là tài liệu RFC số 822 về Internet Email bởi Dave Crocker.

Trang chủ của RFC: http://www.ietf.org/rfc.html

DNS là gì? Tại sao ta lại dùng DNS, DNS làm việc ra sao, tên miền là gì, etc...?

DNS là viết tắt của Domain Name System. Một máy chủ DNS đợi kết nối ở cổng số 53, có nghĩa là nếu bạn muốn kết nối vào máy chủ đó, bạn phải kết nối đến cổng số 53. Máy chủ chạy DNS chuyển hostname bằng các chữ cái thành các chữ số tương ứng và ngược lại. Ví dụ: 127.0.0.1 --> localhost và localhost--->127.0.0.1

Hệ thống "tên đến địa chỉ" (name-to-address) được dùng trước đây khi DNS chưa ra đời, đây thực chất là 1 file trên server. Cấu tạo của 1 file này là 1 table với "hostname" và địa chỉ IP tương ứng, file này được cập nhật và bảo quản bởi Standford Reserch Institute Network Information Center (SRI-NIC). Vài lần 1 tuần, tổ chức này lại cập nhật nội dung file này. Những nguòi quản trị mạng nếu cần sẽ download file này xuống để dùng cho local DNS. Dần dần, số lượng của các trang web trên internet ngày càng nhiều. Cách cũ dùng "name-to-address" trở nên thiếu hiệu quả và tốn thời gian --> DNS ra đời. DNS ko phụ thuộc vào bất cứ 1 server riêng rẽ nào, DNS được phân phát cho nguòi dùng dưới dạng 1 file cơ sở dữ liệu, file này được giữ trên khắp các DNS server trên toàn thế giới. Mỗi DNS server đều tự tìm kiếm một DNS cao hơn khi nhân được yêu cầu về 1 host nào đó ko có trong cơ sở dữ liệu trên máy mình

Máy chủ DNS (DNS Server)

DNS server là 1 máy tính bình thường có thể PC(/MAC) chạy UNIX hoặc nhân bản của Unix (Linux,etc..) và chay một chương trình quản lý domain name gọi là BIND (Berkely Internet Name Domain). DNS server có thể chạy các hệ điều hành khác như Windows, MacOS nhưng thường thì *nix hay được chọn hơn cả vì unix có tính bảo mật cao hơn và cho phép lượng truy cập lớn hơn.

Chương trình quản lý DNS được thiết kế chia làm 2 phần, phần thứ nhất là 1 "daemon" nghe ở cổng 53 đợi kết nối. Phần thứ 2 là để gửi yêu cầu lên một DNS cao hơn nếu local database ko có thông tin mà máy khách yêu cầu. Phần thứ nhất (daemon) trả lời trình duyệt web mỗi khi nhận được yêu cầu. Ví dụ, khi bạn mở Internet Explorer và đánh vào http://www.hackervn.org,/ trình duyệt của bạn sẽ gửi yêu cầu đến 1 máy chủ có dịch vụ DNS gần nhất để tìm IP của http://www.hackervn.org/ vì trình duyệt của bạn cần biết IP máy chủ hiện đang lưu trữ trang web http://www.hackervn.org./ Máy chủ DNS ở ISP của bạn sẽ tìm trong cơ sở dữ liệu, nếu ko tìm thấy địa chỉ IP cho http://www.hackervn.org/ máy chủ chạy DNS này sẽ chuyển sang phần thứ 2 là đưa yêu cầu của máy khách đến 1 máy chủ DNS cao cấp hơn, nhiều dữ liệu hơn để giải quyết.

Định dạng cây của DNS (tree formation)

Một khi DNS server ko thể tìm thấy số IP tương ứng cho 1 hostname trong cơ sở dữ liệu của mình, server đó sẽ gửi yêu cầu đến 1 DNS server khác cao hơn 1 bậc, và DNS server này sẽ lặp lại quá trinh mà DNS server dưới đã làm để tìm địa chỉ IP của 1 host nào đó. Nếu DNS server này vẫn ko tìm thấy thì yêu cầu sẽ lại được gửi đến 1 DNS server khác cao hơn nữa và quy trình này sẽ được tiếp tục cho đến khi nào ra kết quả. Kết quả của yêu cầu này chỉ có thể là "Tìm Thấy" hoặc "Ko tìm thấy". :-) . Đến thời điểm này, chắc bạn đã hình dung ra được cấu trúc của các DNS server như thế nào rồi? Nếu chưa, hãy nhìn vào ví dụ dưới đây:

Ví dụ nhà cung cấp internet của bạn là FPT. Trang web đặt trên máy chủ của FPT là http://www.fpt.vn./ Mặc định, DNS server sẽ là dns.fpt.vn. Bây giờ bạn muốn truy cập http://www.hackervn.org./ dns.fpt.vn sẽ tìm thông tin về host này ở trong cơ sở dữ liệu trên máy chủ DNS ở FPT xem ai đó đã gửi thông tin truy cập về host này chưa. Nếu đia chỉ hackervn ko được tìm thấy ở "local database" hoặc trong bộ nhớ, dns.fpt.vn sẽ đưa yêu cầu này đến 1 DNS server cao cấp hơn, ở đây sẽ là "dns.vn". DNS server này quản lý tất cả các trang có đuôi .vn. Tuy nhiên server này có thể ko có địa chỉ này trong cơ sở dữ liệu nhưng có thể có vì có thể ai đó đã truy cập trang này. Nếu ở đây vẫn ko tìm thấy host/ip cần tìm, DNS server này cuối cùng phải gửi request đến DNS server lớn nhất quản lý tất cả các domain gọi là ".root". Máy chủ chạy .root DNS này là một máy tính rất mạnh, và cơ sở dữ liệu của .root này bao gồm tất cả các loại domain trên toàn thế giới. như .com , .net , .mil, .co.uk, vân vân.....

Khi nào và tại sao DNS bị "bại liệt" ?

Kết quả tìm kiếm 1 trang web có thể lâu hay nhanh tuỳ thuộc vào nhà cung cấp dịch vụ internet của bạn có địa chỉ IP và host đó ko trong cơ sở dữ liệu ở trên máy chủ DNS hay không. Nếu nhà cung cấp dịch vụ Internet có sẵn thông tin bạn cần trong "local DNS database" có lẽ chỉ vài giây là bạn có thể có thể xem đươc trang web còn nếu ko thì sẽ mất 1 khoảng thời gian lâu hơn, tồi tệ nhất là khi bạn nhận được thông báo "Page can not be displayed", có nghĩa là 1 là trang web đó ko tồn tại hoặc là do quá trình "yêu cầu" DNS quá lâu nên browser của bạn "time out" và "giết chết" kết nối. Tuy nhiên bạn có thể Refresh lại trình duyệt, nếu lần trước là do "time out" thì lần này bạn sẽ nhận đươc trang web đó nhanh hơn vì máy chủ DNS của nhà cung cấp dịch vụ Internet của bạn đã cập nhật đươc trang đó trong lần yêu cầu trước khi bạn gửi đến.

Khái niệm về Ping và cách hoạt động?

Ping là 1 khái niệm rât đơn giản tuy nhiên rất hữu ích cho việc chẩn đoán mạng. Tiểu sử của từ "ping" như sau: Ping là tiếng động vang ra khi 1 tàu ngầm muốn biết có 1 vật thể khác ở gần mình hay ko, nếu có 1 vật thể nào đó gần tàu ngầm tiếng sóng âm này sẽ va vào vật thể đó và tiếng vang lại sẽ là "pong" vậy thì tàu ngầm đó sẽ biết là có gì gần mình.

Trên Internet, khái niệm Ping cũng rất giống với tiểu sử của nó như đã đề cập ở trên. Lệnh Ping gửi một gói ICMP (Internet Control Message Protocol) đến host, nếu host đó "pong" lại có nghĩa là host đó tồn tại (hoặc là có thể với tới đươc). Ping cũng có thể giúp chúng ta biết được lượng thời gian một gói tin (data packet) đi từ máy tính của mình đến 1 host nào đó.

Có 1 loại dịch vụ Ping khác gọi là "TCP Ping" và "UDP Ping". Hai dịch vụ này đều đợi kết nối ở cổng số 9 và ghi lại những gì bạn đánh trên màn hình. Dịch vụ này được sử dụng khi người quản trị mạng ko muốn máy chủ của mình nhận những gói tin ICMP(để tránh Denial Of Service) nhưng vẫn muốn để mọi nguòi ping để xem máy chủ của mình "chết" hay "sống".

Số thứ tự (Sequence numbers) là gì?

"Sequence number" là những số xuất hiện trong phần "header" của 1 gói tin TCP. Mục đích của "sequence number" là để các gói tin được nhận theo đúng trình tự như khi chúng được gửi đi. Một trong những phiền toái trong việc truyền dữ liệu qua mạng Internet nói chung và Intranet nói riêng là sự chuyển đổi các gói tin (Packet Switching). Nôm na là như sau, mỗi gói tin đi mỗi con đường khác nhau để tới địa chỉ của host. Gói tin A đi đừong này nhưng gói tin B có khi lai đi đường khác. TCP/IP được thiết kế sao cho mỗi gói tin TCP tìm con đường nào nhanh nhât để đến được đia chỉ đích nhưng con đường này thường là đồng nhất(Với TCP). Gói tin gửi đi phụ thuộc vào tốc độ của đường truyền mà nó đi qua nên những gói tin này ko thể đến nơi cùng 1 lúc, có gói sẽ đến trước có gói sẽ đến sau. Ví dụ gói thứ nhất sẽ đến sau gói thứ 10 chẳng hạn.

Để chắc chắn là máy đích nhận đươc các gói tin theo trình tự để sau này lắp lại thành 1 file hoàn chỉnh, mỗi gói tin TCP "header" bao gồm 1 số thứ tự (sequence number). Nếu ko có số thứ tự này thì máy đích sẽ gần như ko thể lắp ráp các gói tin lại thành một file hoàn chỉnh được, nhất là đối với những file to vài trăm Megabyte.

"Thời Gian Để Sống" (Time To Live)

Như bạn đã biết (có thể ko biết), Internet là một mạng rất rộng lớn. Để đảm bảo các gói dữ liệu đến được máy đích thì quả là một vấn đề. Nếu các gói dữ liệu này đến được chỗ cần đến thì khỏi phải nói, nhưng nếu những gói tin này bị lạc trên đường thì sao?Chính vì thế "Time To Live" ra đời. Khi những gói tin này ko đến được máy đích sau khi đã đi qua số một số router(số này đã được mặc đính trước) sẽ tự phân huỷ.

"Time To Live" chỉ tồn tại trong gói tin TCP. Đây là 1 cách để thủ tục TCP bảo đảm gói tin được gửi đi đến đúng địa chỉ, và để người nhận biết là gói tin vừa gửi đi đã bị mất hoặc thất lạc nếu có gì xảy ra, như vậy gói tin đó sẽ được gửi lại. Time To Live là 1 số tự nhiên, mỗi khi gói tin TCP đi qua 1 router, con số này sẽ giảm đi 1 giá trị, khi số này giảm xuống còn 0, gói tin sẽ tự tiêu huỷ và thông báo ICMP được gửi về thông báo là gói tin vừa gửi ko đến được để máy này gửi lại gói tin vừa thất lạc.

Hầu hết các máy đều để giá trị của gói tin TCP là 32. Các chuyên gia về mạng đưa ra lời khuyên là nên để giá trị mặc định TTL là 64, một số khác lại cho là 128 nhưng 128 có vẻ là hơi nhiều.

Thế nào là kết nối TCP 3 chiều (3 way TCP hand-shake)

TCP là nghi thức kết nối trước, truyền tải dữ liệu sau. Cụ thể là nếu bạn muốn truyền dữ liệu giữa 2 máy tính nối mạng, trước tiên bạn phải thiết lập một số giao

thức giữa 2 máy với nhau để báo cho nhau là đã chuẩn bị cho việc gửi và nhận dữ liệu hay chưa. Quá trình này gọi là kết nối 3 chiều của TCP (TCP 3 ways hand-shake)

Để có thể giúp bạn hiểu rõ ràng hơn về vấn đề này, chúng tôi xin đưa ra ví dụ minh hoạ sau. Chẳng hạn máy tính A muốn thiết lập kết nối TCP đến máy tính B, trước tiên máy tính A sẽ phải gửi 1 gói tin gọi là gói tin với header được đánh dấu SYN (với 1 bit ở TCP header là on) đến B. Gói tin SYN này bao gồm số thứ tự (sequence number). Khi B nhận được gói tin có dấu SYN này từ A, máy B sẽ gửi một gói tin SYN của chính nó và 1 gói tin khác nữa gọi là ACK. Gói tin ACK này thực chất là một gói tin tương tự như SYN nhưng chứa dữ liệu của gói tin SYN mà A gửi cho máy B lúc đầu. Cuối cùng, máy A gửi một gói tin SYN cuối cùng lại cho B như là ở bước thứ 2 khi B trả lời cho A.

(SYN) A -----> B Khi quá trình này hoàn tất, 2 máy tính có thể thiết

lập kết nối và truyền tải dữ liệu cho nhau dưới dạng

TCP

(SYN)+(ACK)A <----- B
(ACK) A -----> B

Chú ý: Truyền tải dữ liệu dưới nghi thức UDP thì ko cần phải thiết lập kết nối trước giống trong TCP. Những gói tin TCP thường đi cùng một đường, qua cùng router tuy nhiên đối với UDP thì do ko thiết lập một kết nối nào cả giữa 2 máy nên mỗi gói tin đều tự tìm các đường khác nhau để đến máy đích, ko có một còn đường nào thống nhất cả.

Khái niệm về "timeout" ?

"Time out" đượoc dùng để miêu tả khoảng thời gian máy A gửi 1 gói tin cho máy B nhưng ko nhân được trả lời từ máy B. Ví dụ khi bạn kết nối vào 1 server chat nào đó chẳng hạn như việtchat, bạn click vào nút connect nhưng sau khoảng 1 phút vietchat server vẫn chưa trả lời. Đây gọi là time out.

Khái Niệm tracert (traceroute) và cách làm việc?

Traceroute là một công cụ để chuẩn đoán mạng rất tốt. Tiện ích này có sẵn ở trong windows(tracert) hoặc unix(traceroute). Tracert dùng TTL(Time To Live) để phát hiện đường đi của gói tin và sau đó ping các router mà gói tin này đã đi qua. Tiện ích này thực sự hữu ích khi bạn muốn kết nối đến một máy chủ nhưng bạn ko tài nào đến được và bạn muốn xem là những router nào trên đường mà gói tin này đã đi cản trở giao thông mạng

Đầu tiên, lệnh tracert gửi một gói tin với giá trị TTL là 1. Gói tín với giá trị TTL = 1 này sẽ bị tiêu huỷ ngay sau khi nó bước qua router đầu tiên, thông báo lỗi sẽ được gửi trả về máy của bạn. Sau đó lại một gói tin TCP khác được gửi đi nhưng lần này với giá trị TTL=2. Như các bạn đã biết, khi đến router thứ 2 gói tin này sẽ bị "chết" và thông báo lỗi sẽ được gửi về máy bạn và cứ thế. Sau khi đã hoàn thành cả một

đoạn đường dài qua tất cả các router mà gói tin cần đi qua, tracert dùng lệnh ping các router trên đường để xem những router nào đã trả lời và mất số lượng thời gian là bao lâu. Như vậy, người dùng có thể tự xem router nào nhanh, router nào cho gói tin đi qua ...vân vân.. Có thể là do chậm hoặc là bị down.

Chú ý:

Trong windows: tracert hostname

Trong unix: traceroute hostname

Khái niệm về HTTP và cách hoạt động

HTTP là viết tắt của cụm từ tiếng anh Hyper Text Transfer Protocol. Đây là một nghi thức dùng cho trình duyệt web (Opera, Internet Explorer....) để giao tiếp với máy chủ Web và hiển thị thông tin. Khi bạn gõ địa chỉ của 1 web-site nào đó vào hộp địa chỉ trong trình duyệt Web và gõ "Enter", việc đầu tiên trình duyệt của bạn sẽ làm là tìm ở máy chủ DNS xem địa chỉ IP của máy chủ chứa trang đó là gì. Sau khi đã tìm thấy địa chỉ IP, trình duyệt web của bạn sẽ tìm cách để kết nối vào cổng (port) mà máy chủ đó dùng cho http(cổng mặc định là 80) và lấy thông tin mà bạn cần hiển thị(ở đây là trang web).

Tip: Bạn có thể chỉnh sửa file host(c:\windows\host) trong win 98 hoặc c:\windows\System32\driver\host để ghi lại những server mà bạn hay truy cập. Như vậy thì sẽ tiết kiệm được nhiều thời gian để tìm IP trên DNS server.

Dưới đây là 2 lệnh căn bản bạn nên biết:

1) "get"...Đây là lệnh trình duyệt dùng để lấy 1 trang web nào đó mà bạn đang yêu cầu. Ví dụ get url HTTP/1.0. url là địa chỉ trang web còn HTTP/1.x là version của dịch vụ HTTP mà trình duyệt của bạn dùng.

2) "post"... Đây là lệnh trình duyệt dùng để gửi 1 file lên trên server.

FTP là gì và cách làm việc

FTP là viết tắt của cụm từ tiếng anh File Transfer Protocol. Đây là nghi thức dùng để truyền tải dữ liệu từ máy này sang máy khác. Điểm lợi của FTP là tính dễ sử dụng, bạn có thể dễ dàng kết nối vào 1 máy chủ FTP và tìm những file bạn muốn miến là những file đó là cho public. Hiện nay trên thế giới có rất nhiều tiện ích FTP dễ dùng như CuteFTP etc...

Chú ý: Bạn có để ý rằng tất cả các nghi thức liên quan đến Internet mà chúng ta đã tìm hiểu trong bản FAQ đều kết thúc bằng từ P (protocol). Và như bạn thấy, thủ tục nào cũng đều liên quan đến việc truyền tải file (upload và download).

Các lệnh và cách sử dụng Telnet

Lệnh

cd ...chuyển thư mục ls hoặc dir ...list các file trong thư mục hiện thời
get ...download file xuống máy bạn
ls ...list file (Unix)
cdup ...chuyển đến thư mục mẹ
put ...upload file lênt máy chủ ở thư mục hiên thời
quit .....ngắt kết nối và thoát
help list các lệnh.

SMTP là gì và cách hoạt động.

SMTP là viết tắt của Simple Message Transfer Protocol. SMTP là một nghi thức của Internet dùng để gửi thư. Khi dùng SMTP để gửi thư, bạn thường phải dùng một chương trình Sendmail(Sendmail Deamon). Có thủ tục khác gọi là QMail nhưng thường thường Sendmail vẫn phổ biến hơn cả mặc dù Sendmaili là một nghi thức gửi thư rất ko an toàn.

Chương trình sendmail có cổng mặc định là 25, cổng này mở để đợi máy khách kết nối vào để gửi thư. SMTP có thể bị kẻ xấu lợi dụng để dùng vào mục đích ko tốt vì SMTP ko dùng hệ thống kiểm tra người dùng. Bạn chỉ cần kết nối vào server và đưa ra địa chỉ nội dung thư là thư đó được gửi đi ko cần biết bạn là ai. Hiện trên thế giới có rất nhiều SMTP server, bạn có thể dùng google để tìm những server này.

Tuy nhiên bạn vẫn có thể khám phá ra bức thư bạn nhận được là thật hay giả bằng cách chỉ cần nhìn vào header của thư đó.

Pop 3 là gì và cách hoạt động

Pop 3 là viết tắt của Post Office Protocol, số 3 là số phiên bản mới hơn của POP. Đơn giản nghi thức này dùng để nhận thư từ POP3 server.

Khi kết nối để nhận thư bằng Outlook, Eudora hay các chương trình e-mail khác để gửi thư, trước tiên chương trình sẽ kết nối đến POP3 server, server này thường đợi kết nối ở cổng mặc định là 110. Bạn nên chú ý là POP3 email khác với Web email, đối với POP3 bạn có thể telnet vào server để check thư trong khi với Webmail thì bạn phải vào hẳn trang web để check(ví dụ Hotmail). Web email thường là chậm hơn so với POP3 email.

POP3 là một nghi thức dễ học nhất trong các nghi thức, đôi khi kiến thức POP3 có thể có lúc hữu dụng. Ví dụ khi bạn bị bomb-mail chẳng hạn, bạn có thể telnet vào POP3 server và xoá những bomb thư đó đi mà ko phải tải chúng xuống máy bạn.

----EOF---