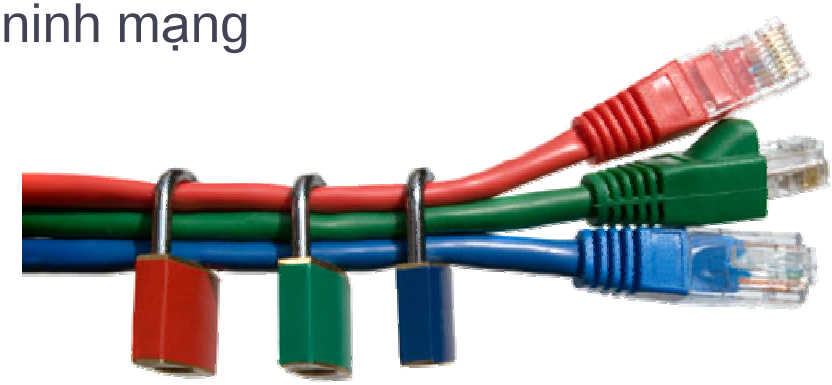
Chương 1

Tổng quan về an toàn hệ thống và an ninh mạng

- Thế nào là an toàn hệ thống và an ninh mạng
- Tấn công trên mạng
- Các phần mềm có hại
- Các yêu cầu của một hệ thống mạng an toàn



Mục tiêu

- Cung cấp cho người học một cái nhìn tổng quan về an toàn mạng và các vấn đề liên quan trong an toàn mạng.
- Sau khi hoàn tất chương, sinh viên có những khả năng:
  - Giải thích được thế nào là an toàn hệ thống và an ninh mạng.
  - Phân loại và trình bày được các mối đe dọa đối với hệ thống máy tính và hệ thống mạng.
  - Trình bày được các kỹ thuật tấn công trên mạng gồm: tấn công thăm dò, tấn công truy cập, tấn công từ chối dịch vụ.
  - Hiểu và phân loại được các phần mềm có hại và cách thức hoạt động của từng loại phần mềm có hại.
  - Mô tả được các yêu cầu cơ bản của 1 hệ thống an toàn mạng: chứng thực, phân quyền và giám sát.

Phần 1

Khái niệm về an toàn hệ thống và an ninh mạng

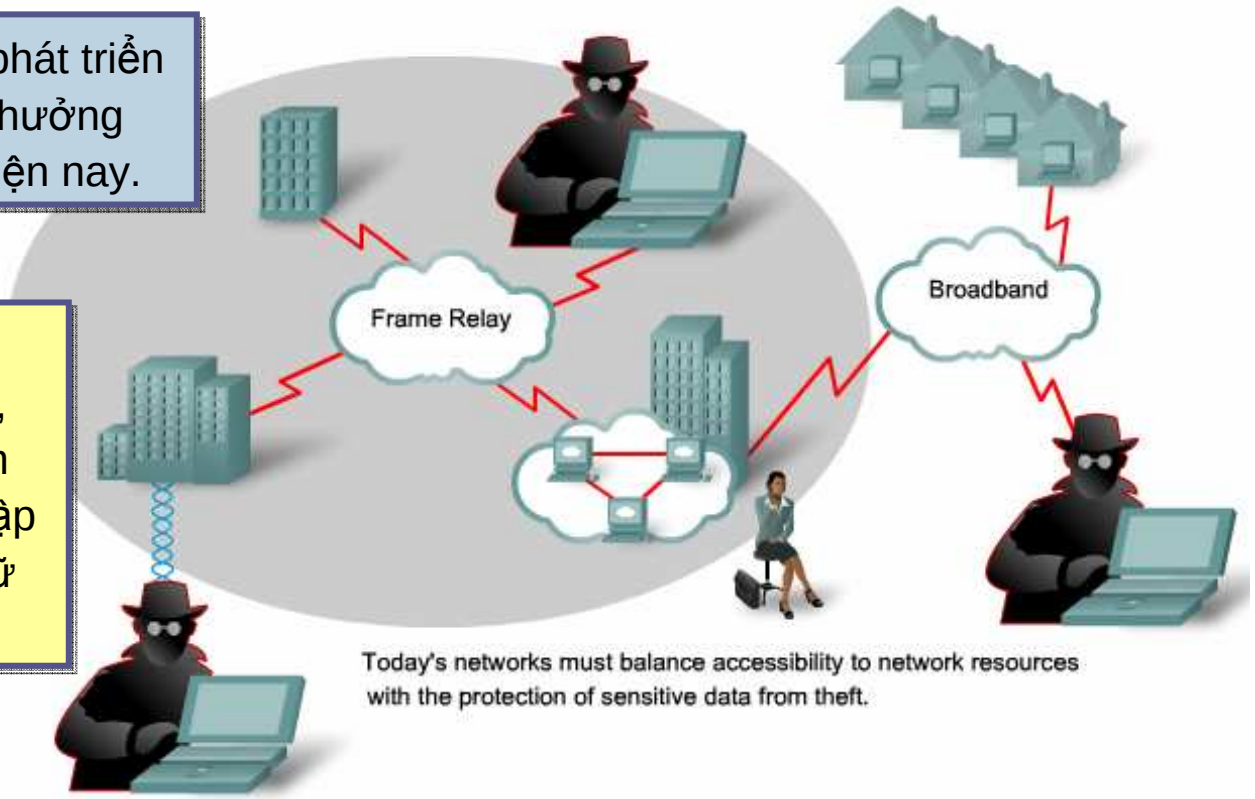
- Tại sao an toàn mạng là cần thiết?
- Thế nào là an toàn hệ thống và an ninh mạng?

Khái niệm về an toàn mạng?

- Tại sao an toàn mạng là cần thiết?

Mạng máy tính ngày càng phát triển cả về tầm vóc và mức ảnh hưởng của nó đối với cuộc sống hiện nay.

Nếu an ninh mạng không được quan tâm đúng mức, sẽ có nhiều vấn đề nghiêm trọng xảy ra như: xâm nhập bất hợp pháp, đánh cắp dữ liệu, tấn công lừa đảo, …



Khái niệm về an toàn mạng?

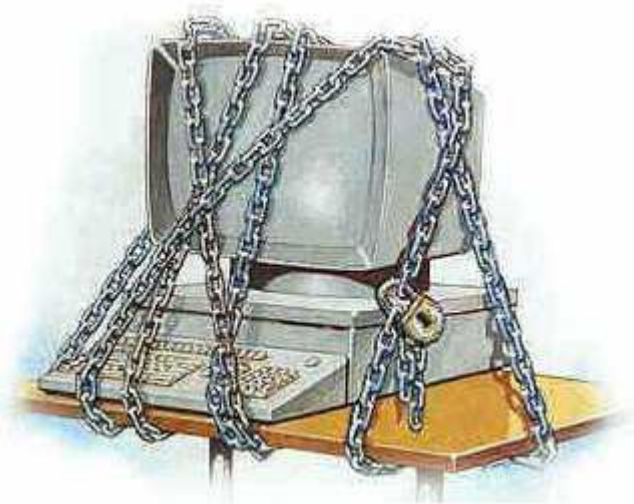
- Thế nào là an toàn mạng (network security)?

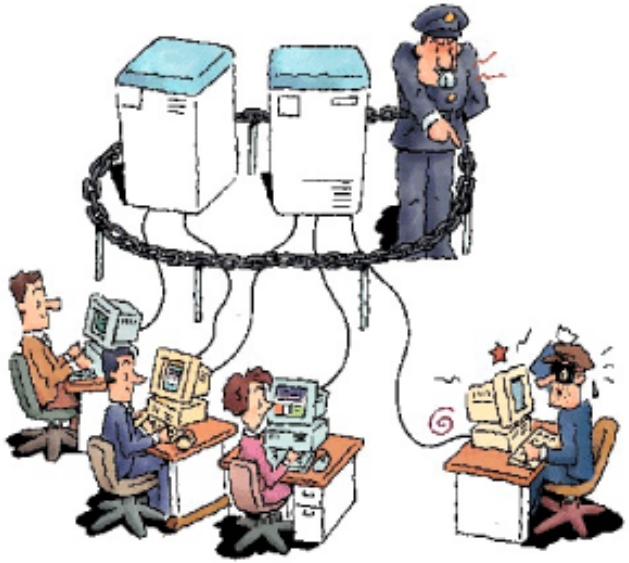
An toàn *(an ninh, bảo mật - security):* là một quá trình liên tục bảo vệ 1 đối tượng khỏi các tấn công.

An toàn thông tin *(information security):* là khả năng **bảo vệ** đối với **môi trường thông tin** kinh tế xã hội, đảm bảo cho việc **hình thành**, **sử dụng** và **phát triển** vì lợi ích của mọi công dân, mọi tổ chức và của quốc gia.

Khái niệm về an toàn mạng?

- Thế nào là an toàn mạng (network security)?





An toàn máy tính *(computer security):* là an toàn cho tất cả các tài nguyên của hệ thống máy tính:

- Phần cứng vật lý: CPU, màn hình, bộ nhớ, máy in, CDROM, các thiết bị ngoại vi khác, …
- Phần mềm, dữ liệu, thông tin lưu trữ bên trong.

An toàn mạng *(network security):* là an toàn thông tin trong không gian của mạng máy tính.

Khái niệm về an toàn mạng?

- Mục tiêu cần đạt được của một hệ thống an toàn mạng:

- **Sự bảo mật** (*confidentiality*): bảo đảm dữ liệu khỏi sự truy xuất hay theo dõi.
- **Tính toàn vẹn** (*integrity*): bảo đảm dữ liệu không bị thay đổi hay phá hoại.
- **Tính sẵn dùng** (*availability*): bảo đảm tính thông suốt của hệ thống và tài nguyên

Phần 2

Tấn công trên mạng

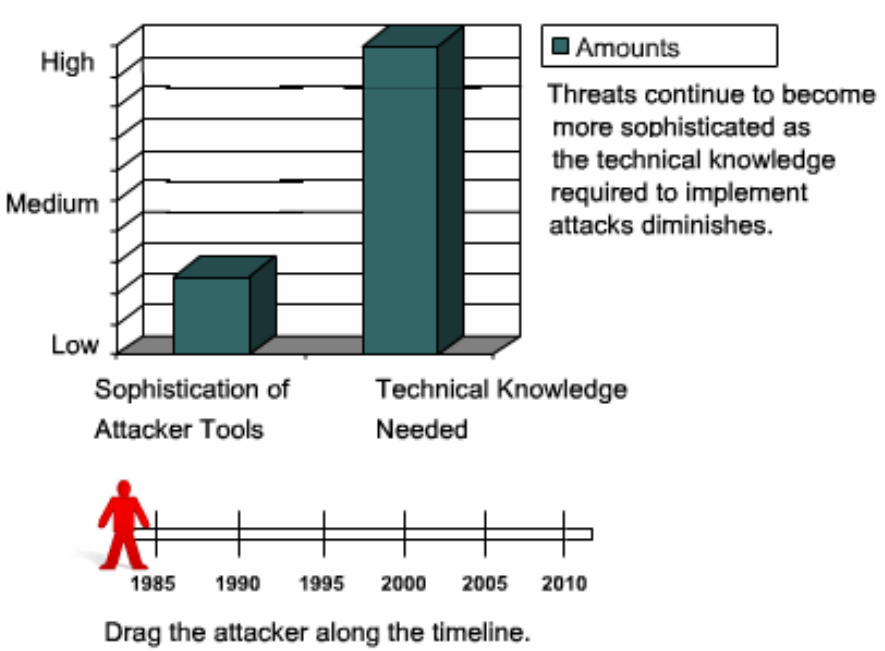
- Các mối đe dọa (threat) của một hệ thống máy tính.
- Phân loại những kẻ tấn công.
- Các hình thức tấn công: do thám, truy cập và từ chối dịch vụ.

Tấn công trên mạng

- Các mối đe dọa của hệ thống mạng máy tính

Có nhiều tác nhân có thể là mối **đe dọa** (threat - còn gọi là **hiểm họa** hay **mối nguy hại**) cho một mạng máy tính.

Có thể chia các mối đe dọa (threat) thành các dạng sau:
- Đe dọa có tổ chức và không tổ chức
- Đe dọa từ bên ngoài và từ bên trong
- Đe dọa chủ động và thụ động .
- Đe dọa cố ý và vô tình .



Các mối đe dọa cho hệ thống mạng

- Đe dọa có tổ chức và không tổ chức

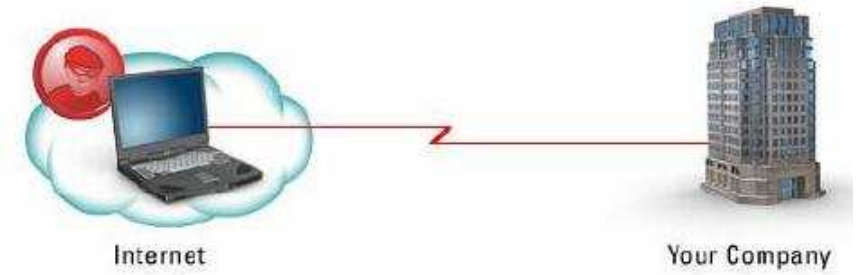
Đe dọa có tổ chức (structured threat) là de dọa được hoạch định trước vào 1 mục đích nhất định và lâu dài.
Các đe dọa này đến từ những hacker thành thạo và có động cơ rõ rệt.

Đe dọa không tổ chức (unstructured threat) là đe dọa mang tính tức thời và là kết quả của những hacker đơn lẻ chưa có kinh nghiệm, thường chỉ dùng các công cụ có sẵn được công khai trên Internet để thử nghiệm.

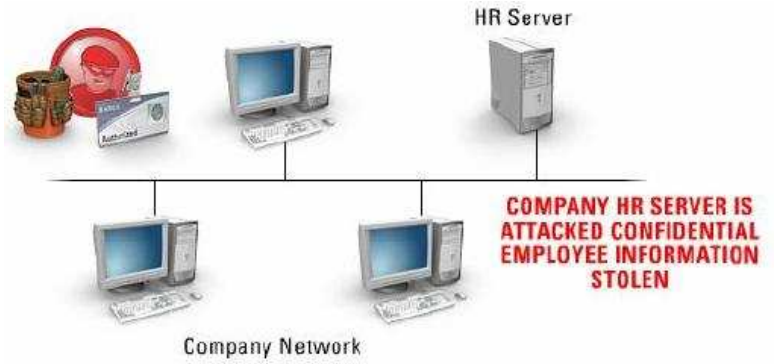
Các đe dọa có tổ chức thường sẽ được che dấu rất khó phát hiện

Các mối đe dọa cho hệ thống mạng

- Đe dọa từ bên ngoài và từ bên trong



• Xuất phát từ các cá nhân hoặc tổ chức **bên ngoài hệ thống mạng**.
• Không có quyền truy xuất vào hệ thống máy tính và hệ thống mạng.
• Chỉ đột nhập vào từ Internet hay bằng đường Dial-up thông qua RAS.



• "70% các vấn đề có liên quan đến bảo mật thường đến từ bên trong mạng".
• Xảy ra từ một ai đó **có quyền truy xuất trong nội bộ mạng**.

Ngăn chặn các đe dọa từ bên trong cũng quan trọng như các đe dọa đến từ bên ngoài.

Các mối đe dọa cho hệ thống mạng

- Đe dọa chủ động (active) - thụ động (passive) và đe dọa cố ý (intentional) - vô tình (unintentional)

Đe dọa chủ động: có thể sửa đổi thông tin hoặc thay đổi tình trạng hoạt động của 1 hệ thống
VD: thay đổi bảng vạch đường của 1 Router.

Đe dọa thụ động: không có thay đổi dữ liệu của hệ thống.
VD: nghe trộm thông tin trên đường truyền.

Đe dọa cố ý: các tấn công tinh vi có sử dụng các kiến thức hệ thống đặc biệt.
VD: cố tình xâm nhập mạng trái phép.

Đe dọa vô tình: một sự kiện ngẫu nhiên có thể gây hại cho hệ thống.
VD: chế độ đặc quyền tự động được login.

Tấn công trên mạng

- Hacker

• **Hacker** (intruder, attacker) là kẻ dùng kiến thức bản thân để thâm nhập, tấn công hệ thống máy tính hay mạng máy tính.
• Đa số hacker đều rất am tường về hoạt động của máy tính và mạng máy tính.

Hacker mũ trắng (white hat): xâm nhập có ý tốt. Chẳng hạn: nhà bảo mật, lập trình viên, chuyên viên mạng.

Hacker mũ đen (black hat): thâm nhập có mục đích xấu như: phá hoại, đánh cắp thông tin, ...

Hacker mũ xám (gray hat): đôi khi là hacker mũ trắng, đôi khi là mũ đen.

Hacker mũ xanh (blue hat): chuyên gia lập trình tài năng, được các công ty lớn mời về làm việc để chuyên tìm lỗi.

Cracker ="Criminal Hacker" (hacker tội phạm)

Về nguyên tắc nói chung mọi Hacker đều là xấu và hành động của họ là trái với pháp luật.

Tấn công trên mạng

- Khái niệm về tấn công

Chúng ta có thể gọi tất cả **các dạng có hại** cho hệ thống máy tính là "tấn công".

Các tấn công có thể xuất phát từ:
- các công cụ được thiết kế sẵn.
- khai thác các điểm yếu của hệ thống.

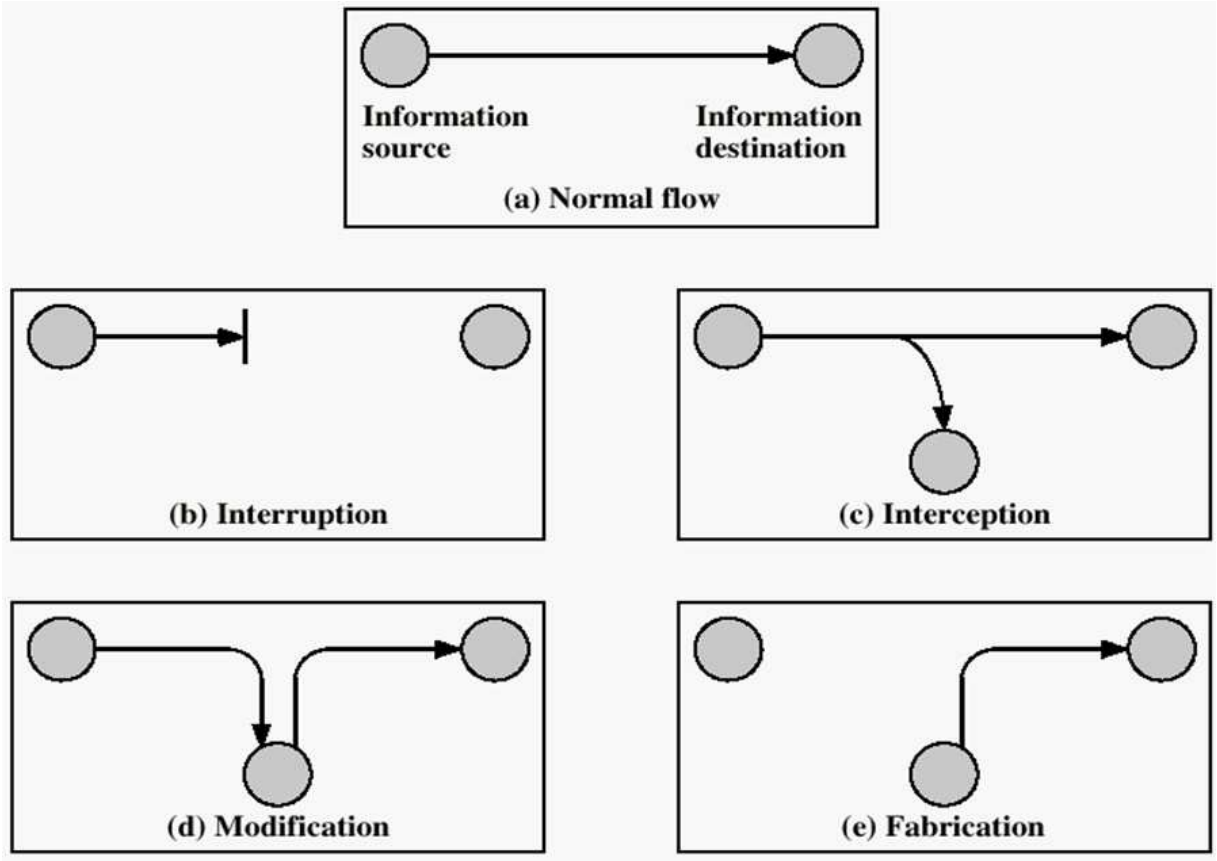
Tấn công có thể gây ra:
- hư hỏng dữ liệu hoặc ngưng trệ hoạt động hệ thống
- không làm hư hại cho dữ liệu và hệ thống (chẳng hạn ăn trộm thông tin) nhưng tác hại có thể lớn hơn.

Có thể phân chia tấn công ra làm 3 loại chính:
1. Do thám (reconnaissance)
2. Truy cập (access)
3. Từ chối dịch vụ (denial of service - DoS)

Tấn công trên mạng

- Khái niệm về tấn công

Các hình thức tấn công trên mạng



Tấn công do thám (Reconnaissance)

- Khái niệm

Tấn công do thám là loại tấn công không phải với mục đích chiếm đoạt hệ thống mà chỉ tìm kiếm thông tin để có thể khai thác sau này

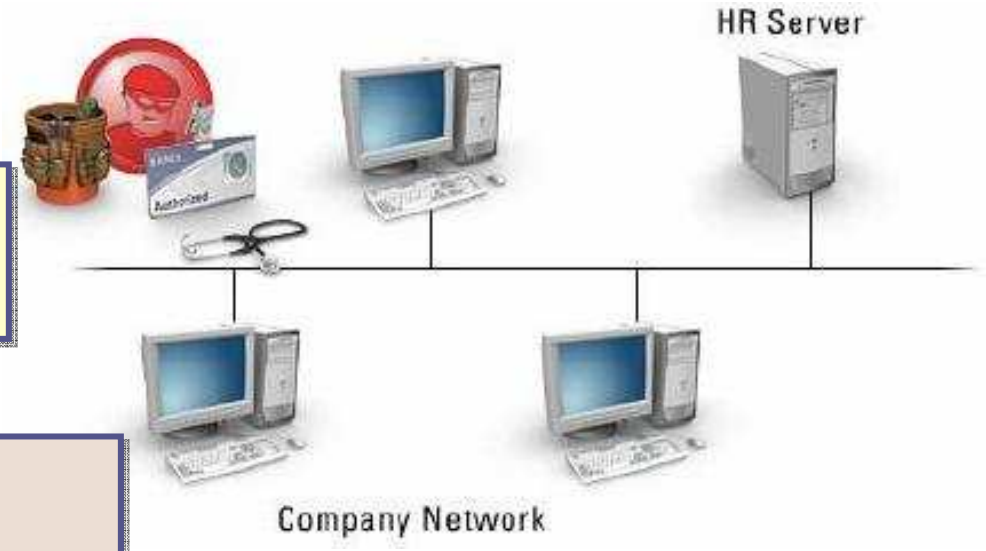
Các kỹ thuật do thám thông dụng:
1. Nghe lén
2. Quét địa chỉ IP
3. Quét cổng
4. Quét tránh né
5. Xác định hệ điều hành

Các thông tin cần ghi nhận:
- Địa chỉ IP
- Các dịch vụ mạng đang sử dụng
- Cổng của các ứng dụng nào đang mở
- Hệ điều hành đang sử dụng
- Phiên bản Web server nào đang sử dụng
- …

Tấn công do thám

- Kỹ thuật nghe lén (sniffer)

Packet sniffer là 1 thiết bị (hay chương trình) dùng để nghe trộm trên đường truyền.



Để nghe lén được, cần phải:

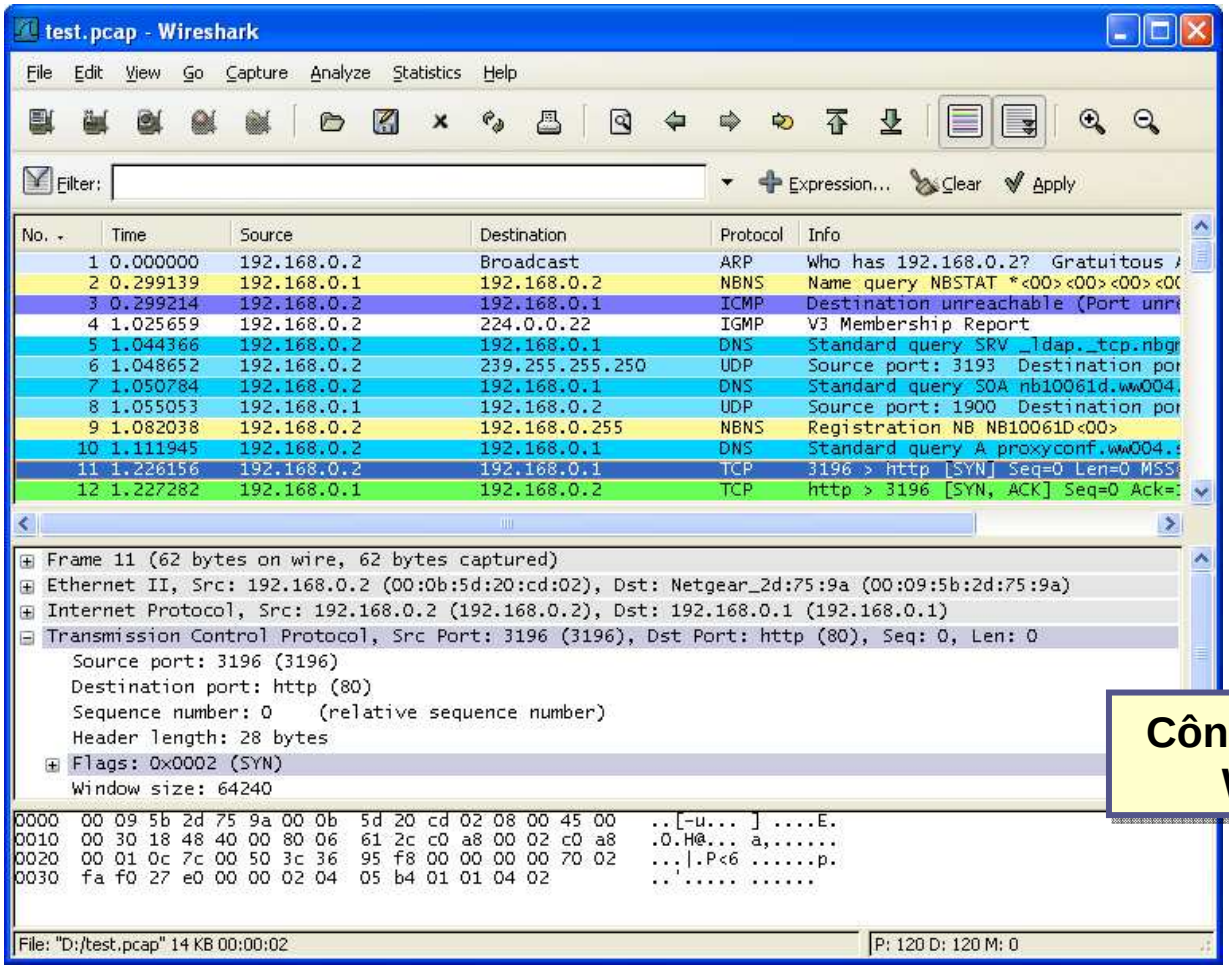
- Có kết nối vật lý đến đường truyền
- Có quyền nhận thông tin :
  - + môi trường Hub
  - + trong cùng khu vực WLAN
  - + dùng thiết bị đặc biệt cho WAN
- Phải có bộ giải mã (decode) để chuyển các bit 0,1 thành thông tin có thể hiểu được.

Các sniffer thông dụng:

- Ngrep
- Ethereal
- Wireshark
- Packet Inspector
- Dsniff

Tấn công do thám

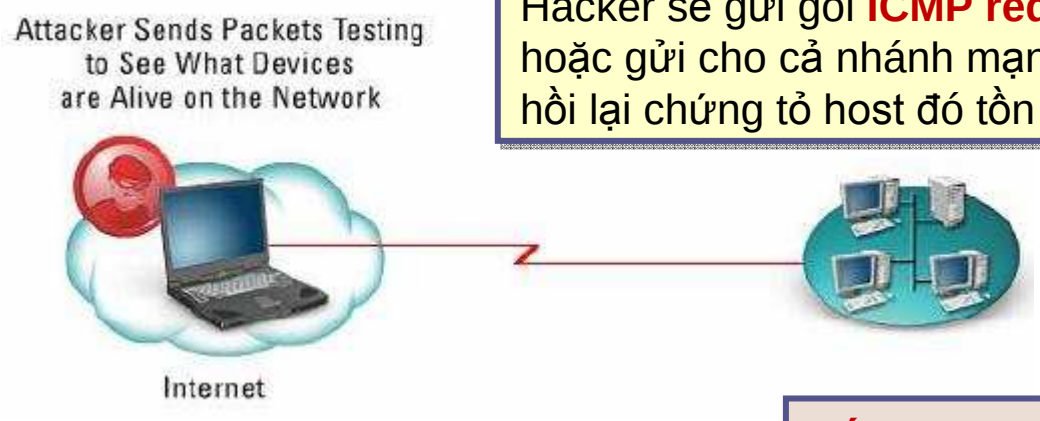
- Kỹ thuật nghe lén (sniffer)



Công cụ nghe lén Wireshark

Tấn công do thám

- Kỹ thuật quét địa chỉ (Ping sweep)



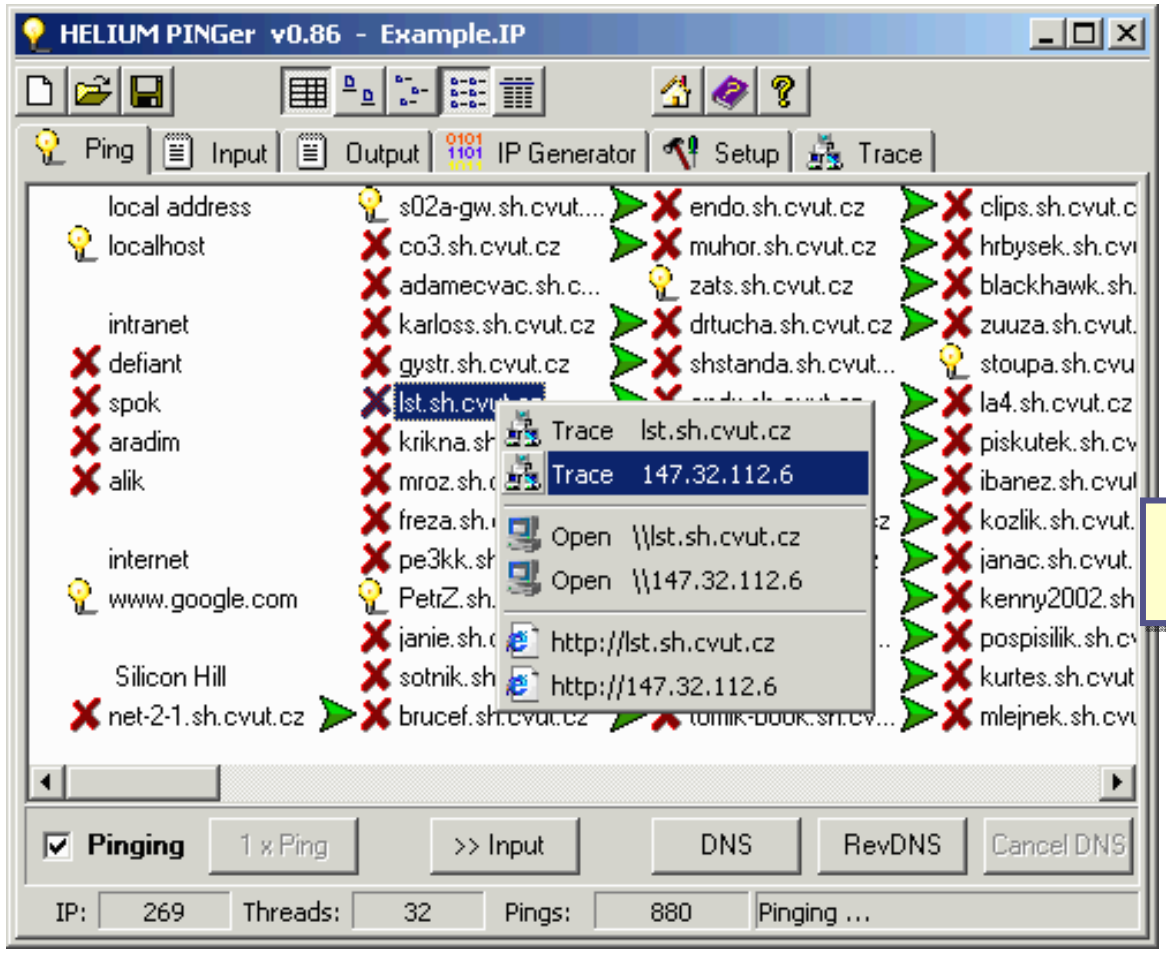
Hacker sẽ gửi gói **ICMP request** đến địa chỉ đích hoặc gửi cho cả nhánh mạng đích. Host nào phản hồi lại chứng tỏ host đó tồn tại và đang hoạt động.

Các công cụ quét địa chỉ thông dụng:
- Fping
- Network Sonar
- Ping sweep
- Pinger

Nếu host không trả lời, chứng tỏ:
- Địa chỉ đó không tồn tại
- Host đó đang tắt
- Host đó hoặc hệ thống mạng đó chặn (block) ICMP.

Tấn công do thám

- Kỹ thuật quét địa chỉ (Ping sweep)

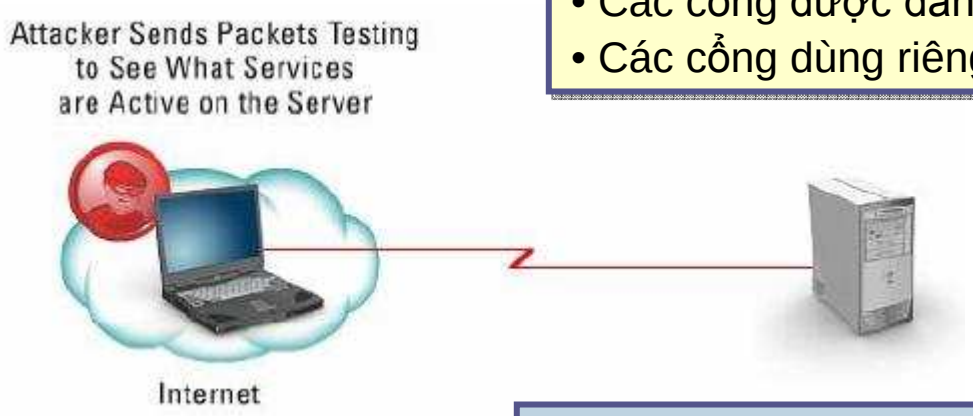


Công cụ quét địa chỉ Helium Pinger

Tấn công do thám

- Kỹ thuật quét cổng (port sweep)

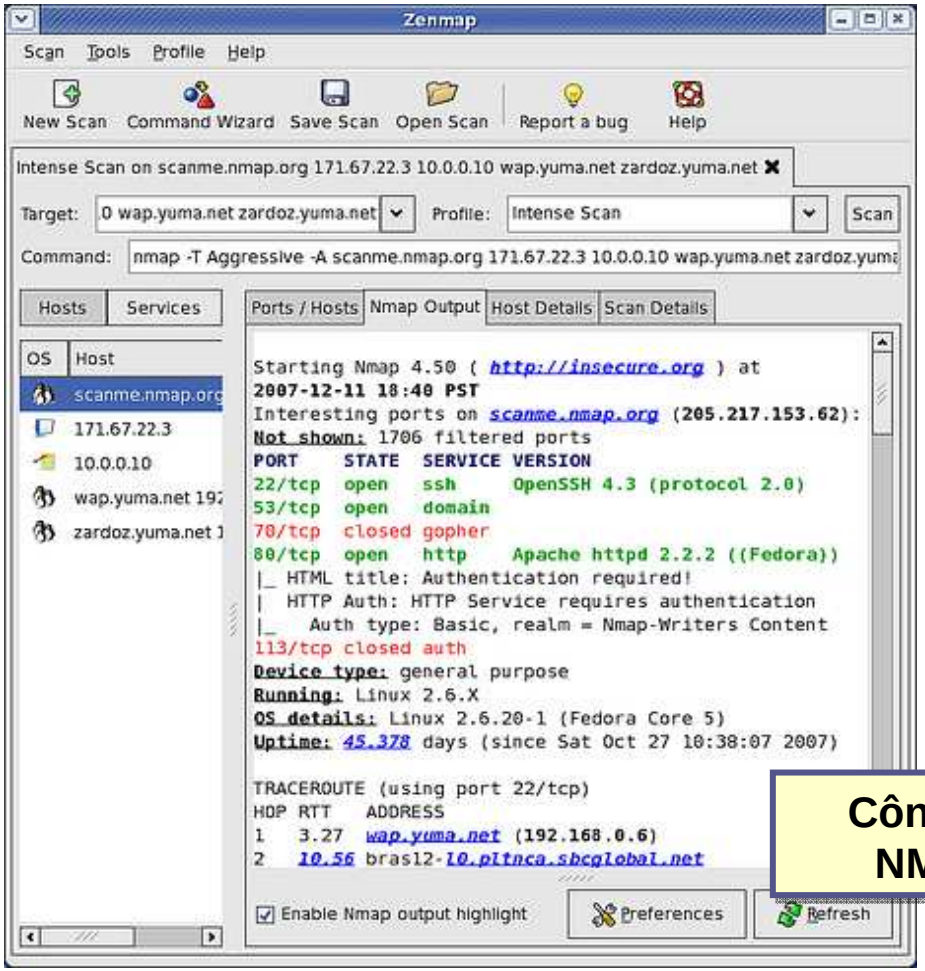
Mỗi dịch vụ mạng đều được gán với ít nhất 1 cổng:
- Các cổng thông dụng (well-known port): 0 – 1023
- Các cổng được đăng ký (registered port): 1024 – 49151
- Các cổng dùng riêng (private port): 49152 - 65535



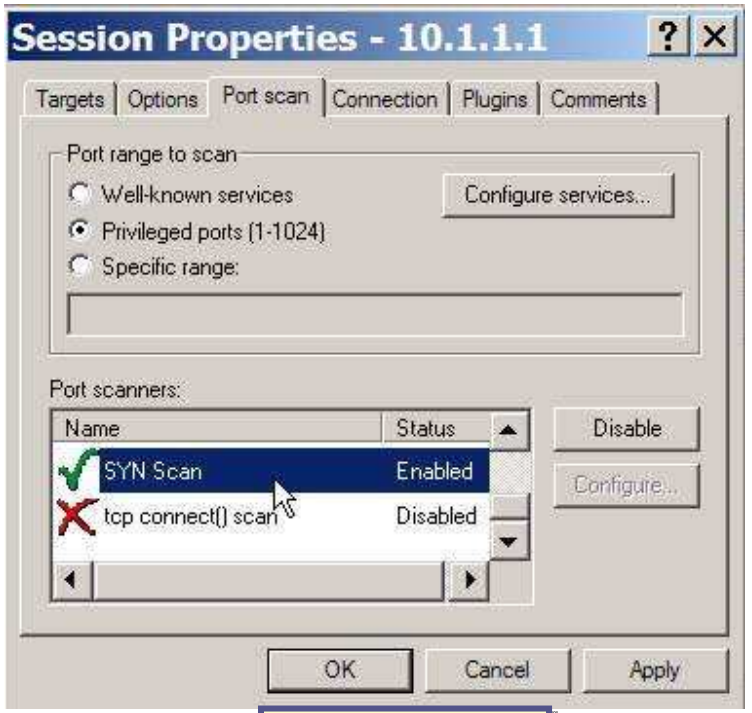
Các công cụ quét cổng thông dụng:
- Nmap
- Nessus
- IPEye
- SuperScan

Tấn công do thám

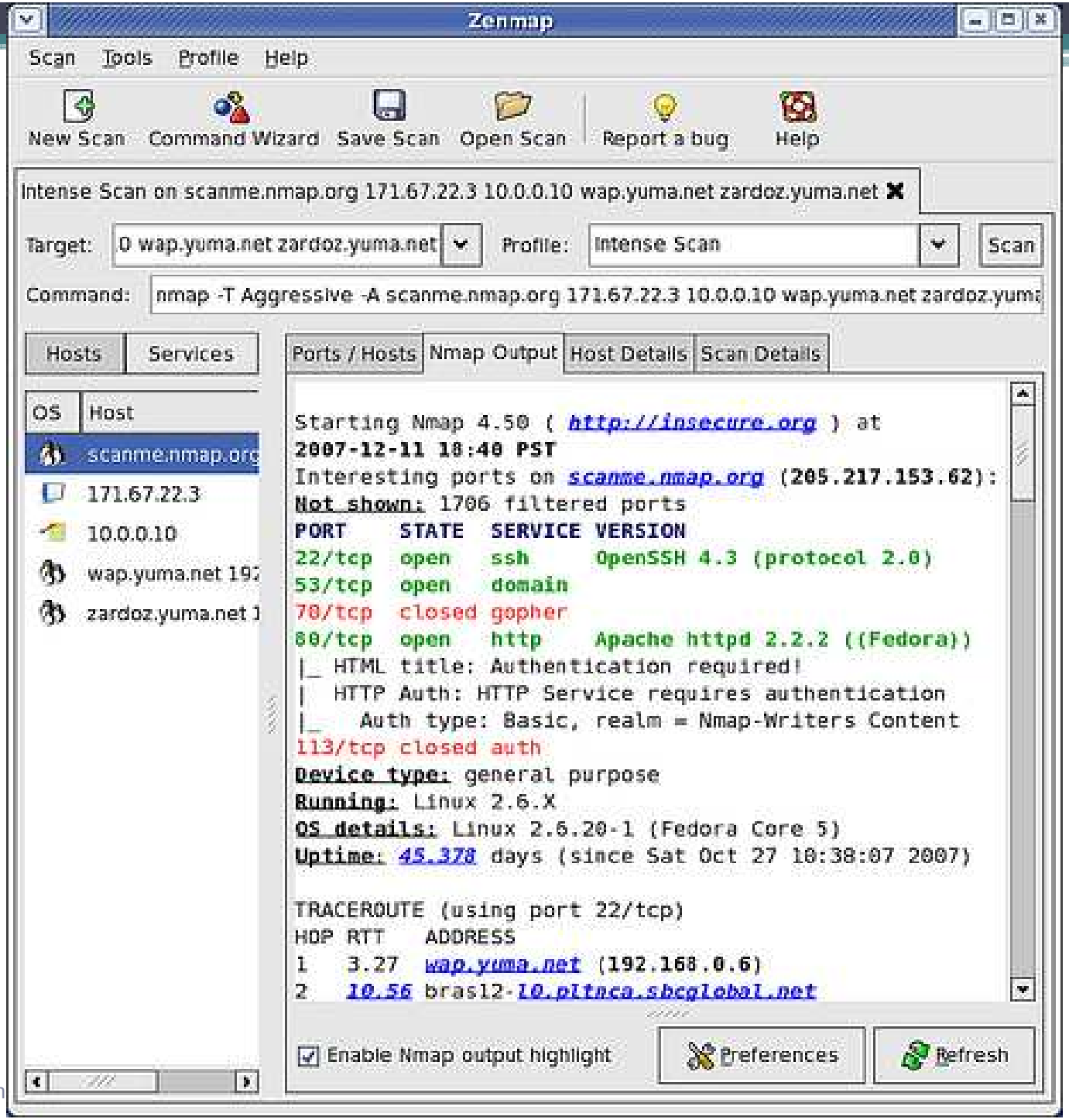
- Kỹ thuật quét cổng (port sweep)



Công cụ NMap

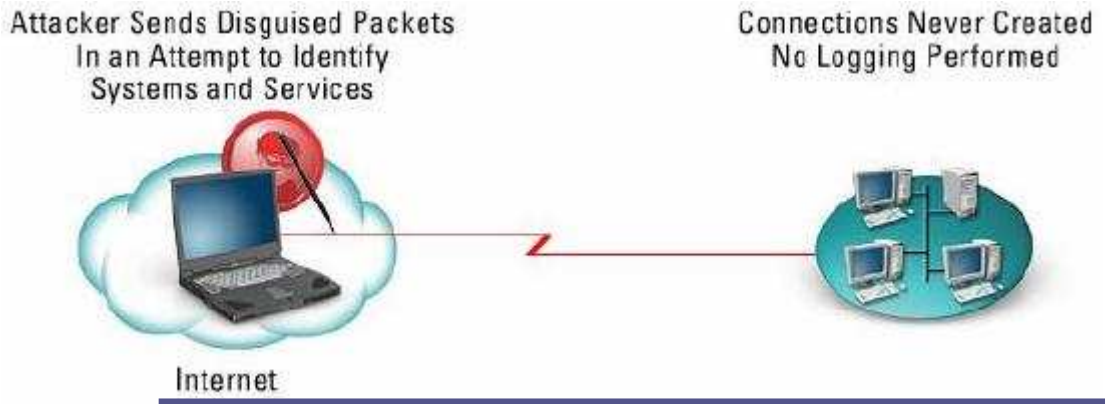


Công cụ Nessus


Zenmap
Scan Tools Profile Help
New Scan
Command Wizard
Save Scan
Open Scan
Report a bug
Help
Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net
Target: 0 wap.yuma.net zardoz.yuma.net
Profile: Intense Scan
Scan
Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma
Hosts
Services
OS
Host
scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 19
zardoz.yuma.net 1
Ports / Hosts
Nmap Output
Host Details
Scan Details
Starting Nmap 4.50 (http://insecure.org) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 4.3 (protocol 2.0)
53/tcp open domain
70/tcp closed gopher
80/tcp open http Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
| HTTP Auth: HTTP Service requires authentication
|_ Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)
TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
1 3.27 wap.yuma.net (192.168.0.6)
2 10.56 bras12-l0.pltnca.sbcglobal.net
Enable Nmap output highlight
Preferences
Refresh

Tấn công do thám

- Kỹ thuật quét có tránh né (Evasive sweep)



Để tránh lưu lại các log file khi nối kết, hacker có thể dùng kỹ thuật quét lén hay quét có che dấu nối kết

Kỹ thuật quét tránh né là quét mà **không tạo ra nối kết đến hệ thống** đó:

• Gửi đến máy tính đích các gói tin được gán cờ FIN trong TCP header (có nghĩa là đóng nối kết với host).

• Nếu máy tính đích **có** cài dịch vụ mạng đó: sẽ gửi thông báo lỗi .

• Nếu máy tính đích **không** cài dịch vụ mạng đó: sẽ bỏ qua gói trên.

Các công cụ quét có tránh né thông dụng là: Nmap, IPEye, SuperScan và AWSPS

Tấn công do thám

- Kỹ thuật xác định hệ điều hành (OS identification)

Biết được hệ điều hành nào đang cài đặt trên máy tính đích, hacker có thể liệt kê ra được danh sách các lỗ hổng và điểm yếu để có thể xâm nhập vào đó

Do việc cài đặt bộ giao thức TCP/IP trên từng loại hệ điều hành là khác nhau nên hiện nay hacker dựa vào đó để xác định loại hệ điều hành cài đặt trên máy tính đích.

Các công cụ có thể dò tìm hệ điều hành là:
Nmap, Queso

Tấn công truy cập (access attack)

- Khái niệm

Tấn công truy cập là loại tấn công chiếm lấy tài nguyên trên hệ thống đích như file, mật khẩu, quyền điều khiển, …

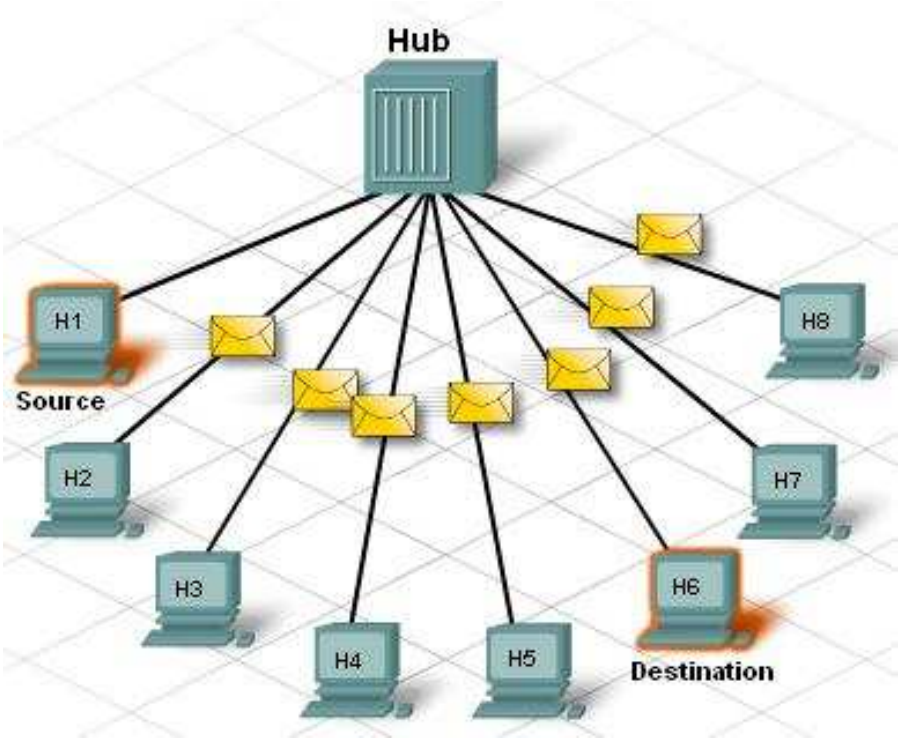
Sau khi tấn công thăm dò để nắm được các thông tin cơ bản về hệ thống đích, hacker sẽ tấn công trực tiếp vào hệ thống gọi là **tấn công truy cập**

Các kỹ thuật tấn công truy cập thông dụng:

1. Nghe lén
2. Sử dụng lại
3. Cướp giao dịch
4. Kẻ đứng giữa
5. Cổng sau
6. Đánh lừa
7. Khai thác lỗi
8. Tấn công mật khẩu

Tấn công truy cập

- Kỹ thuật nghe lén



• Sniffer "bắt" tất cả các gói tin đi đến nó, bất kể là địa chỉ đích có phải là gửi cho nó hay không.
• Chỉ có thể thực hiện trong môi trường mạng dùng Hub .

Gặp khó khăn khi chuyển qua môi trường mạng dùng switch hiện nay.

Tấn công truy cập

- Kỹ thuật nghe lén trong môi trường switch

Làm tràn bảng CAM (CAM table flooding):
Hacker sẽ gửi rất nhiều địa chỉ MAC giả đến switch cùng 1 lúc cho đến khi bảng này đầy. Khi đó Switch hoạt động như 1 Hub.

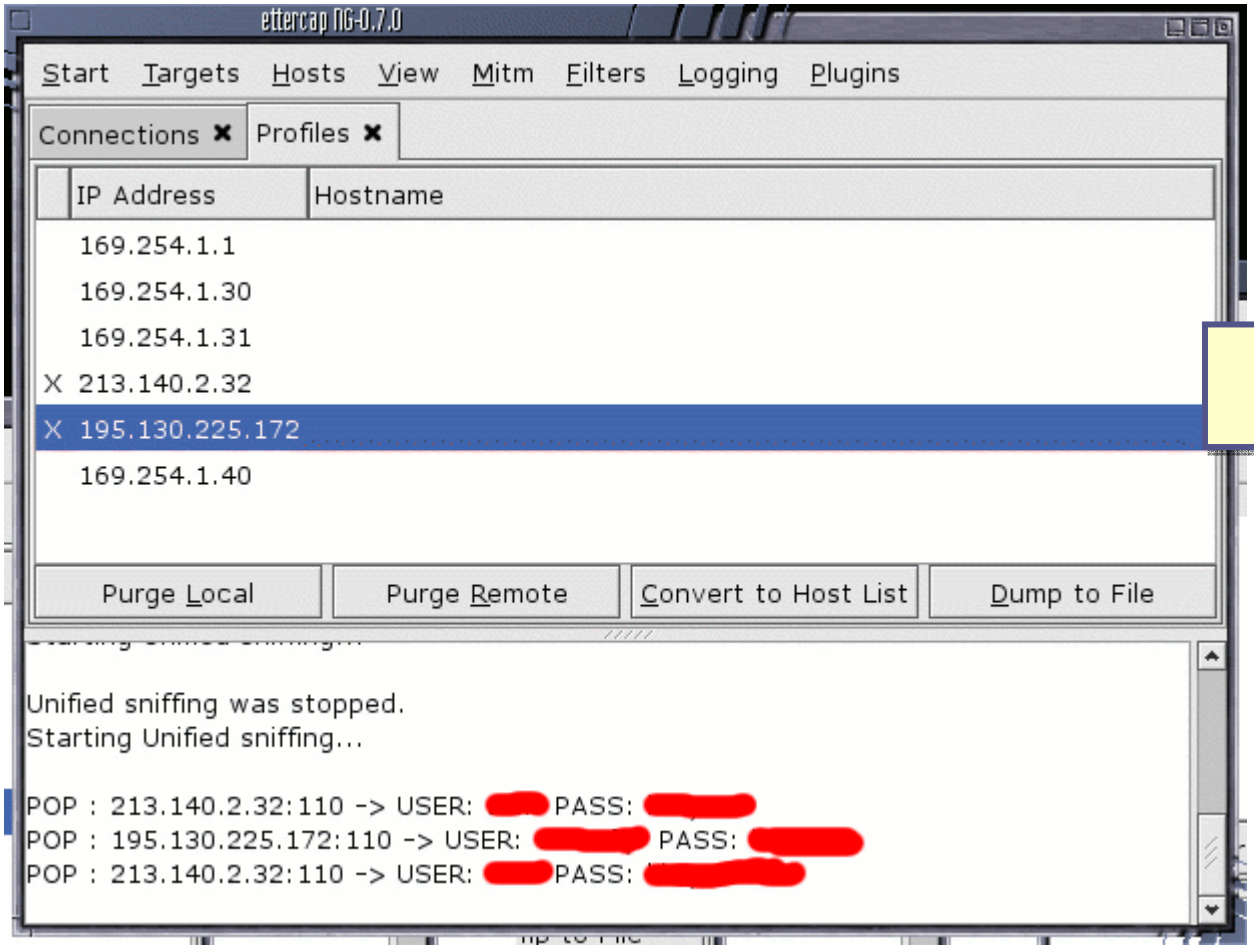
Đặt trùng MAC (MAC duplicating):
- Dùng các công cụ để thay đổi địa chỉ MAC của mình giống như địa chỉ MAC của hệ thống đích.
- Gửi các ARP Reply cho switch để switch hiểu nhầm cổng nối với máy tính có cài Sniffer chính là cổng nối với hệ thống đích.

Giả dạng ARP (ARP Spoofing): Sniffer sẽ giả dạng Gateway của mạng bằng cách gửi các gói ARP Reply cho các máy khác trong mạng LAN. Từ đó các máy này sẽ chấp nhận địa chỉ MAC của sniffer thay cho MAC của Gateway

Giả dạng DNS (DNS Spoofing):
Hacker sẽ liên tục gửi các DNS Reply giả cho hệ thống nguồn để cung cấp địa chỉ IP của mình thay cho địa chỉ DNS của hệ thống đích.

Tấn công truy cập

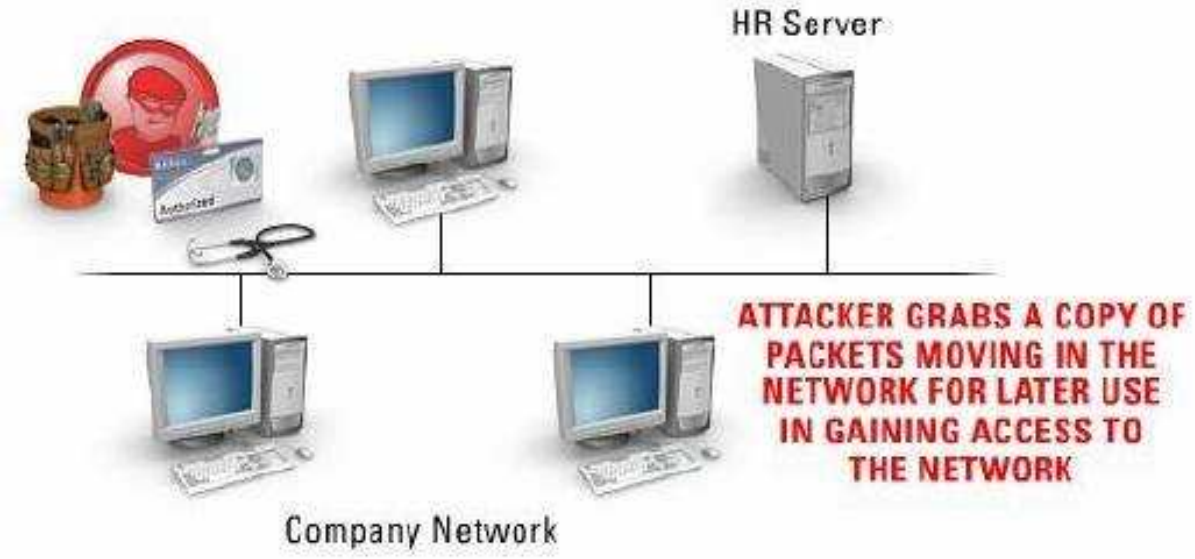
- Kỹ thuật nghe lén trong môi trường switch



Công cụ Ettercap

Tấn công truy cập

- Kỹ thuật tấn công sử dụng lại (Replay)



Hacker sẽ dùng 1 kỹ thuật tấn công (như nghe lén) để lấy được các thông tin quan trọng (chẳng hạn như username và password), **ghi nhận** và **lưu trữ** lại để có thể **dùng cho tấn công sau này**.

Tấn công truy cập

- Kỹ thuật cướp giao dịch (Session hijacking)

Kỹ thuật **tấn công cướp giao dịch** là hacker sẽ nắm quyền điều khiển một giao dịch đang diễn ra và loại bỏ truy cập từ người dùng hợp pháp.

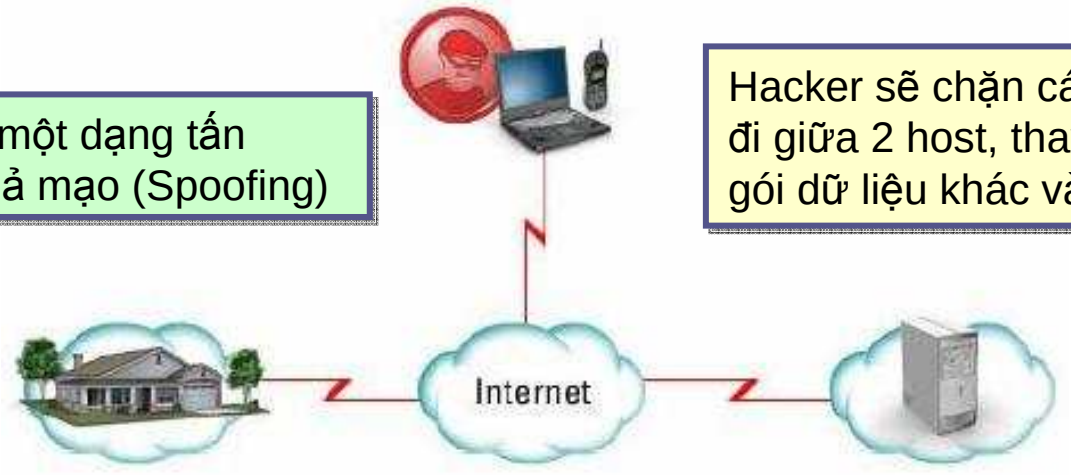
Thực hiện được khi hacker đã nắm bắt được các thông tin chứng thực của người dùng (chẳng hạn cookie) để có thể chiếm được điều khiển của người dùng hợp pháp trong khi người dùng này đã đăng nhập vào hệ thống.

Một số công cụ cướp giao dịch thông dụng là: Juggernaut, ttywatcher, jhijack

Tấn công truy cập

- Kỹ thuật kẻ đứng giữa (Man-in-the-middle)

Đây là một dạng tấn công giả mạo (Spoofing)



Hacker sẽ chặn các gói dữ liệu gửi đi giữa 2 host, thay thế bằng những gói dữ liệu khác và gửi chúng đi

• Thường được thực hiện trên tầng ứng dụng như các dịch vụ Telnet, Rlogin, SMTP, FTP, HTTP, …
• Cách khác là can thiệp vào Router giữa đường đi của 2 host để chuyển gói theo ý mình.

Một số công cụ có thể dùng tấn công dạng Man-in-the-middle là: Ettercap, Burp Suite.

Tấn công truy cập

- Kỹ thuật cổng sau (Backdoor)

Backdoor là một chương trình được hacker cài đặt vào máy nạn nhân để có thể truy cập vào trong thời gian sau cho dù lần xâm nhập trước đó đã bị phát hiện ra.

Các cách thực hiện:
- Tạo thêm 1 dịch vụ mới có tên rất "hệ thống".
- Gở bỏ 1 dịch vụ ít sử dụng và cài đặt backdoor với chính tên đó.
- Có 2 chương trình:
  + Server: cài trên máy nạn nhân
  + Client: sử dụng để điều khiển.

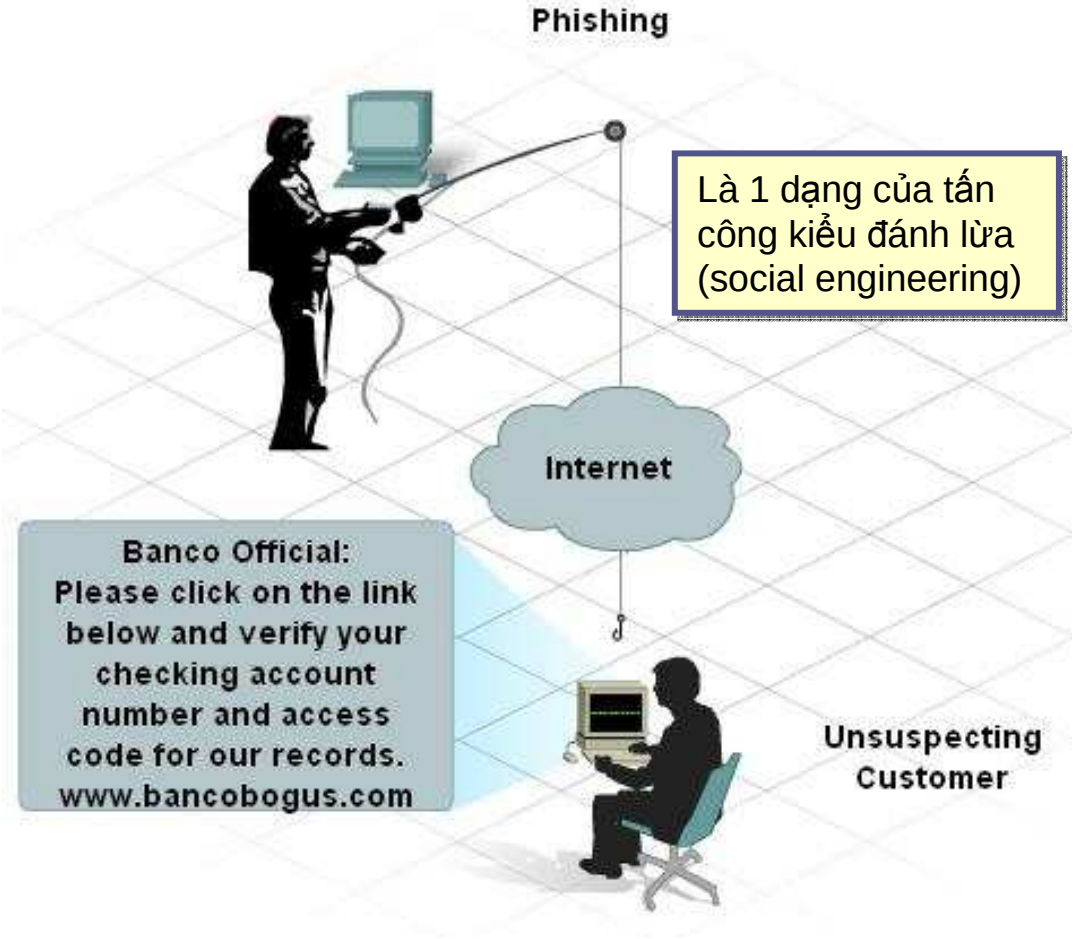
Một số ví dụ điển hình của Backdoor là: BackOrifice , NetBus, Subseven.

Tấn công truy cập

- Kỹ thuật đánh lừa (Social Engineering)

Tấn công truy cập

- Kỹ thuật lừa đảo (Phishing)



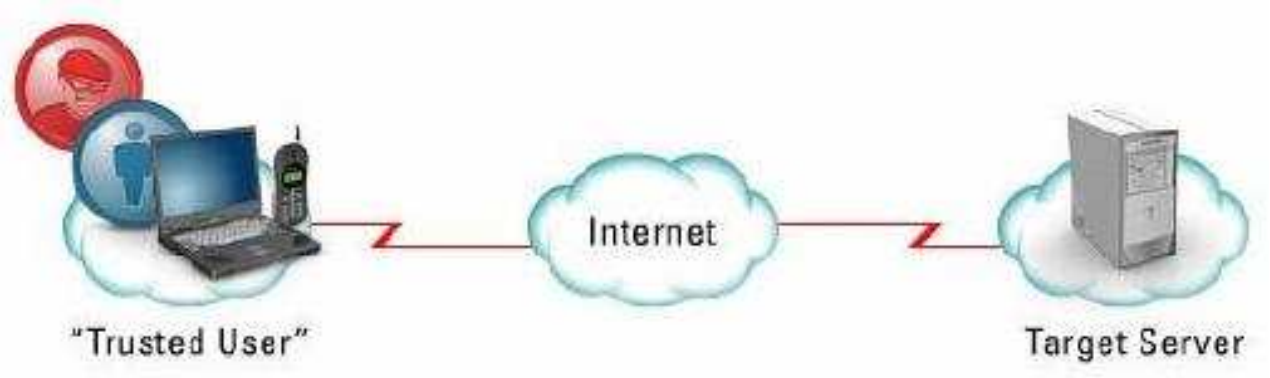
Là 1 dạng của tấn công kiểu đánh lừa (social engineering)

•Hacker gửi 1 email đến người dùng mục tiêu và cung cấp cho họ 1 đường link đặc biệt.
• Thoạt nhìn đường link này giống như đường dẫn đến địa chỉ của website thực của tổ chức đó, nhưng thật ra lại dẫn dắt đến 1 site giả mạo.

Hiện nay, các trình duyệt , phần mềm an ninh mạng đã cung cấp sẵn các tính năng dùng để chống phishing.

Tấn công truy cập

- Kỹ thuật giả dạng (Spoofing)

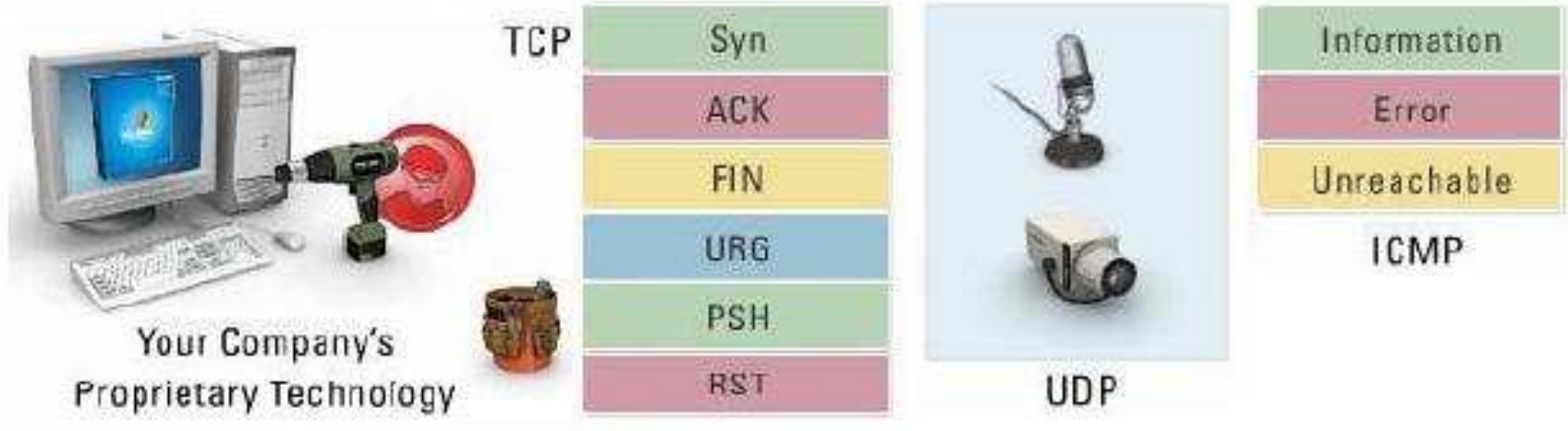


Hacker sẽ đóng vai một máy tính khác truy cập vào mạng và nhận những thông tin đúng ra phải đến máy tính kia.

Các cách giả dạng:
- Giả dạng DNS
- Giả dạng ARP
- Giả dạng gói tin IP: không dễ dàng.

Tấn công truy cập

- Kỹ thuật khai thác (Exploitation)



Hacker có thể tấn công hệ thống bằng cách khai thác :
- Điểm yếu của công nghệ
- Điểm yếu của giao thức: TCP/IP, UDP, ICMP, SNMP, SMTP, ...
- Lỗi của hệ điều hành mạng khi chưa cài đặt các bản vá.

Tấn công truy cập

- Kỹ thuật làm tràn bộ đệm (buffer overflows)

Tác giả của sâu Morris

• Được biết đến đầu tiên vào năm 1988 trong sâu Morris (khai thác lỗi dịch vụ fingerd trong Unix).
• Năm 2001, sâu Code Red khai thác lỗi tràn bộ đệm của IIS 5.0
• Năm 2003, sâu SQLSlammer khai thác lỗi tràn bộ đệm trên SQLServer 2000.

Lỗi tràn bộ đệm là một lỗi lập trình có thể **gây ra một ngoại lệ truy nhập bộ nhớ máy tính** và chương trình bị kết thúc, hoặc khi người dùng có ý phá hoại, họ có thể lợi dụng lỗi này để phá vỡ an ninh hệ thống.

Theo nghiên cứu của Sophos thì hơn 28% lỗi bảo mật hiện nay là lỗi tràn bộ đệm.

Tấn công truy cập

- Kỹ thuật làm tràn bộ đệm

Phần tử A (8 byte) Phần tử B (2 byte)

A	A	A	A	A	A	A	A	B	B
0	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**3**

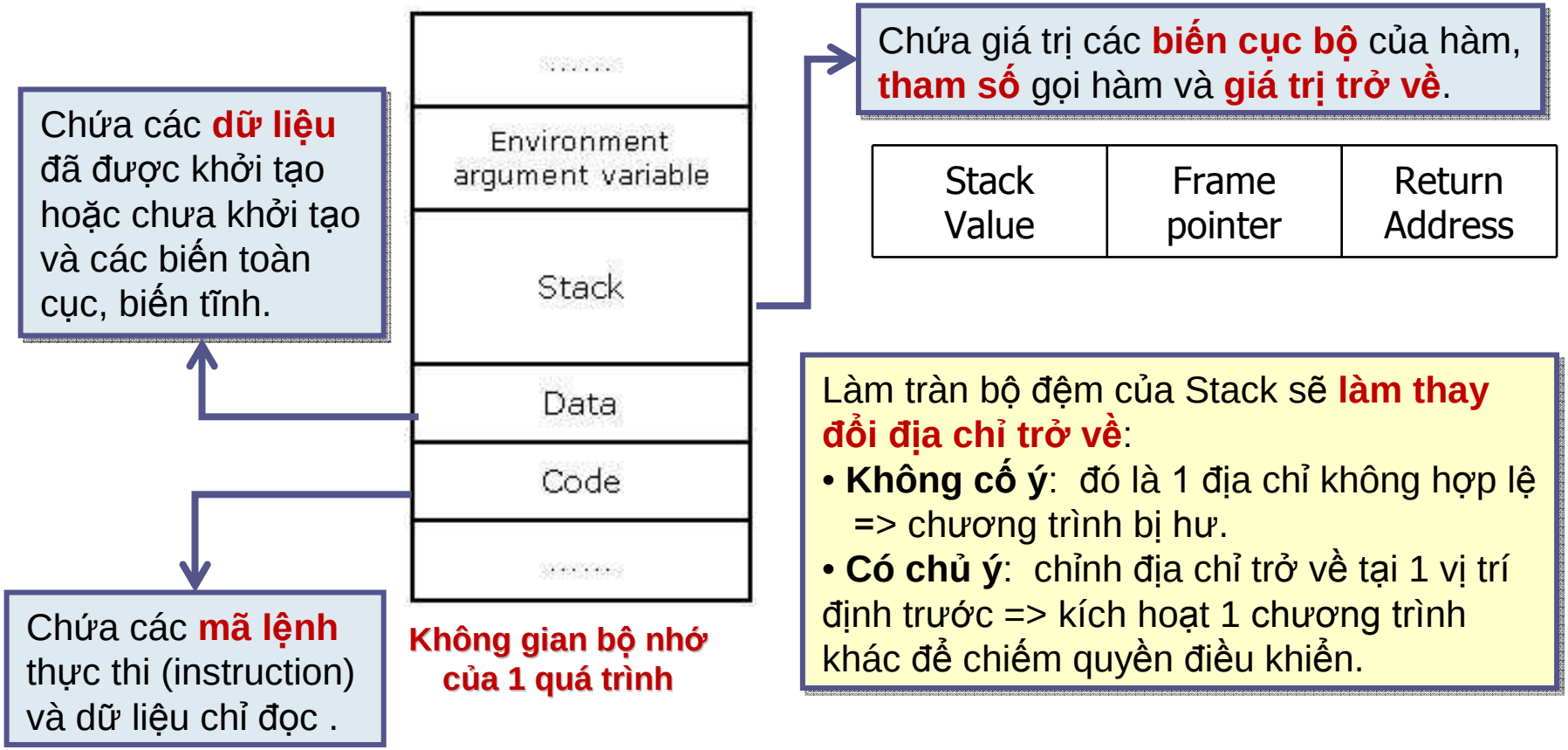
Ghi 1 chuỗi "CNTT-DHCT" vào bộ đệm của A

A	A	A	A	A	A	A	A	B	B
C	**N**	**T**	**T**	**-**	**D**	**H**	**C**	**T**	**\0**

Do lỗi tràn bộ đệm trên A, giá trị của B bị thay đổi dù đây không phải là ý muốn của người lập trình.

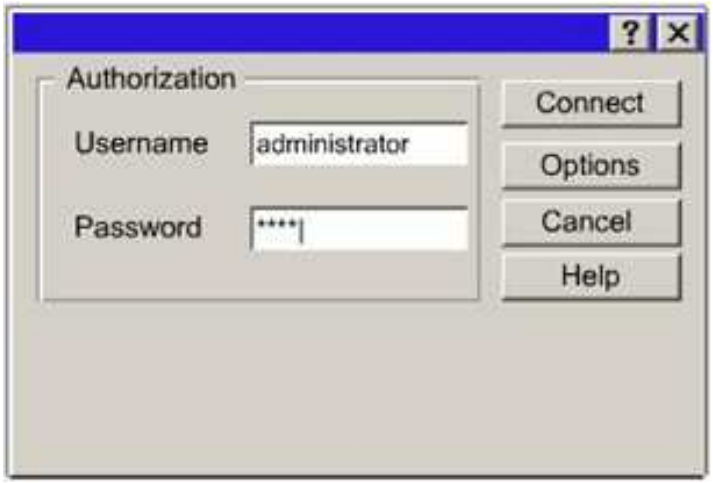
Tấn công truy cập

- Kỹ thuật làm tràn bộ đệm



Tấn công truy cập

- Kỹ thuật tấn công mật khẩu (password attack)



Một số lỗi thường gặp khi đặt mật khẩu:

- Không đổi mật khẩu mặc định
- Mật khẩu quá ngắn
- Mật khẩu quá thông dụng
- Mật khẩu có liên quan đến thông tin cá nhân của người dùng như địa chỉ, tên con, tên bạn, ngày sinh, …

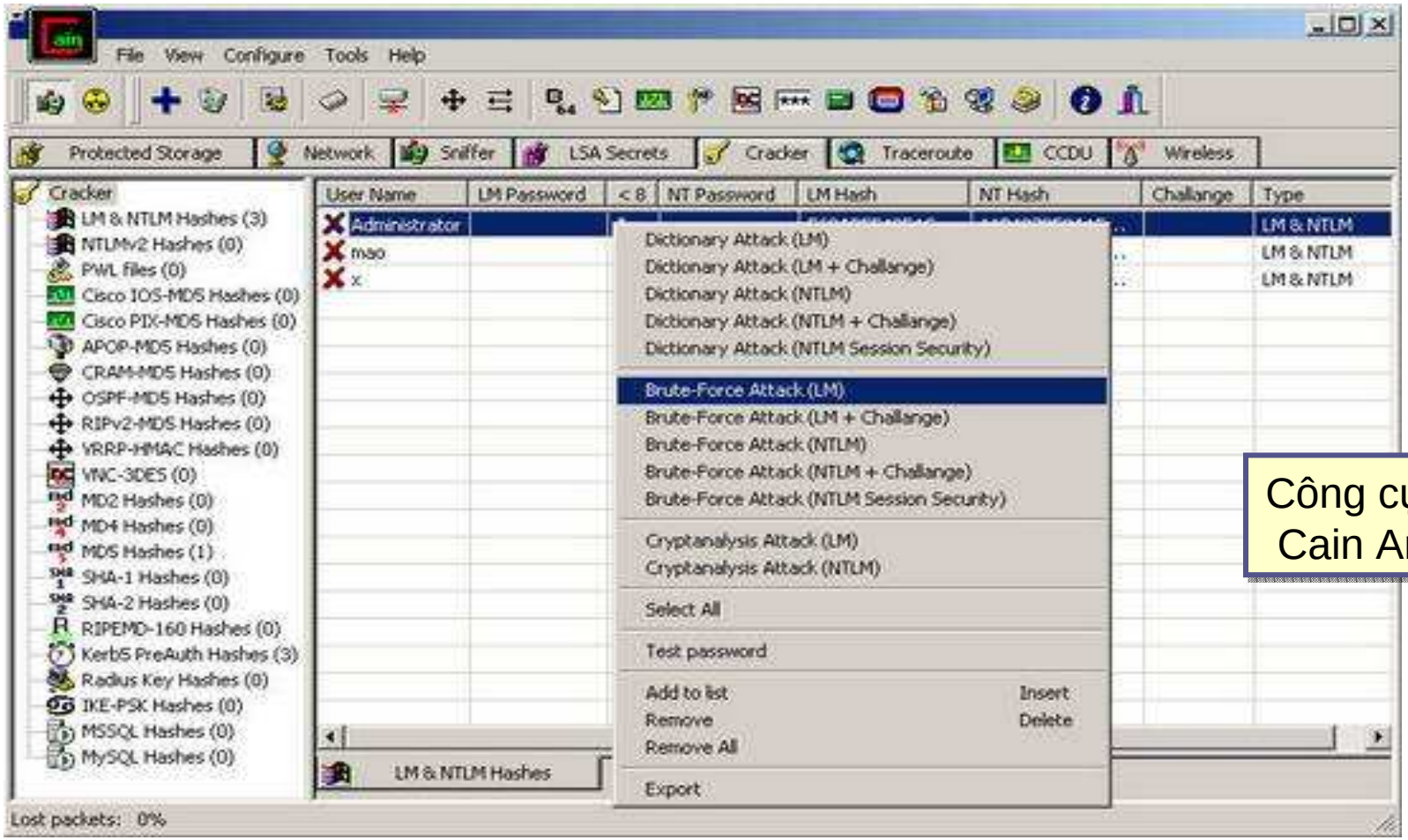
Các phương pháp tấn công mật khẩu:

- Nghe lén trên đường truyền.
- Dự đoán
- Dò tìm theo từ điển *(Dictionary-based)*
- Dò tìm dạng vét cạn *(Brute Force).*

Một số công cụ thông dụng để tấn công mật khẩu là: L0phtCrack, Brutus, Hydra, Cain And Abel, John the Ripper ...

Tấn công truy cập

- Kỹ thuật tấn công mật khẩu (password attack)



Công cụ
Cain And Abel

Tấn công truy cập

- Kỹ thuật tấn công SQL Injection

Lợi dụng **lỗ hổng trong việc kiểm tra dữ liệu nhập** vào trong các ứng dụng web và các thông báo lỗi của hệ QTCSDL để tiêm vào (inject) và **thi hành các câu lệnh SQL bất hợp pháp**.

```
<FORM METHOD=POST ACTION="Execlogin.asp">
 Username: <INPUT TYPE="text" NAME="fUSERNAME"><br>
 Password:  <INPUT TYPE="password" NAME ="fPASSWORD"> <br>
 <INPUT TYPE="submit">
</FORM>
```

login.htm

```
<% Dim vUsername, vPassword, strSQL
   vUsername = Request.Form("fUSERNAME")
   vPassword  = Request.Form("fPASSWORD")
   strSQL= "SELECT * FROM  T_USERS  WHERE USR_NAME= ' " & vUsername &_
           " ' AND USR_PASS = ' " & vPassword  & " ' "
  ..............
%>
```

Execlogin.asp

Tấn công truy cập

- Kỹ thuật tấn công SQL Injection

```
<% Dim vUsername, vPassword, strSQL
   vUsername = Request.Form("fUSERNAME")
   vPassword  = Request.Form("fPASSWORD")
   strSQL= "SELECT * FROM  T_USERS  WHERE USR_NAME= ' " & vUsername &_
           " ' AND USR_PASS = ' " & vPassword  & " ' "
  ..............
%>
```

Execlogin.asp

Nếu nhập vào trong cả 2 ô Username và Password nội dung là: **' OR ' ' = '**

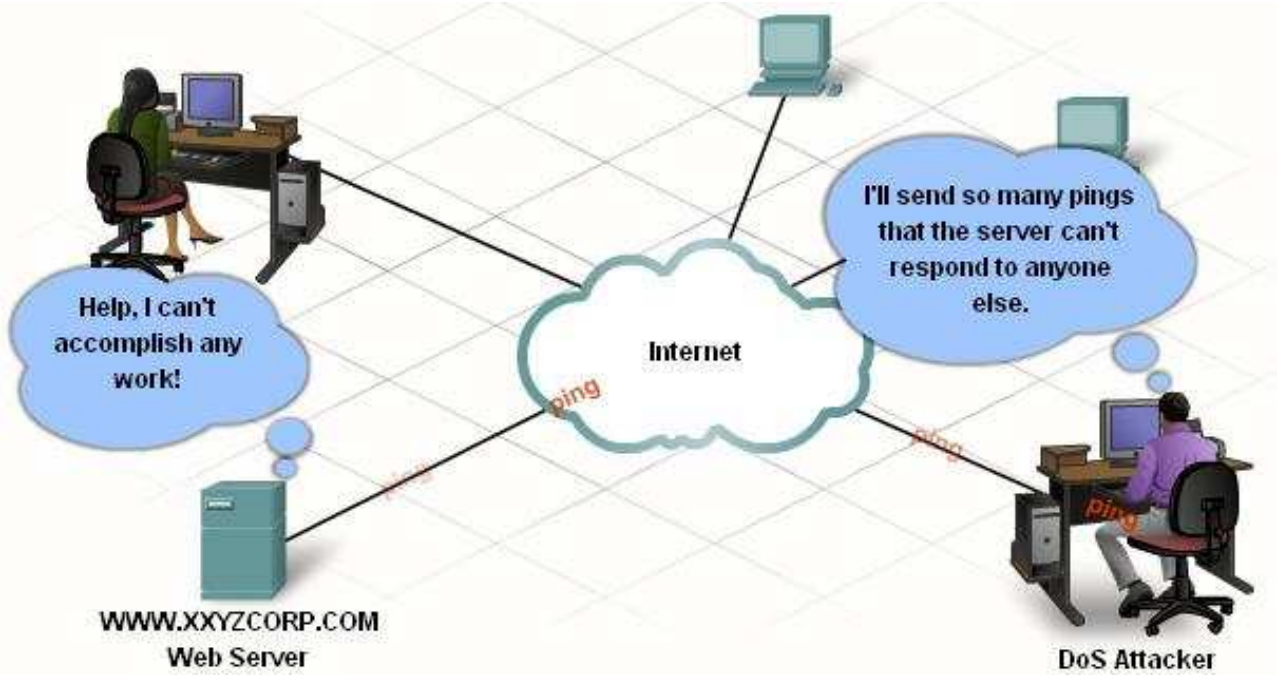
```
SELECT * FROM T_USERS WHERE USR_NAME= '' OR '' = ''
                      AND   USR_PASS = '' OR '' = ''
```

Liệt kê tất cả các record trong bảng T_USERS

Dùng các tài khoản này để đăng nhập vào 1 cách dễ dàng

Tấn công từ chối dịch vụ (DoS)

- Khái niệm

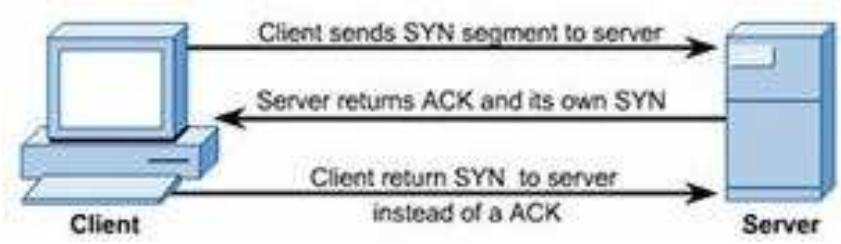


Là tấn công phá hoại chứ không phải muốn lấy được thông tin.

Tấn công bằng từ chối dịch vụ DoS có thể mô tả như hành động **ngăn cản những người dùng hợp pháp khả năng truy cập và sử dụng vào một dịch vụ** nào đó. Nó bao gồm làm **tràn ngập mạng**, **mất kết nối với dịch vụ**… mà mục đích cuối cùng là Server **không thể đáp ứng được các yêu cầu sử dụng dịch vụ** từ các Client.

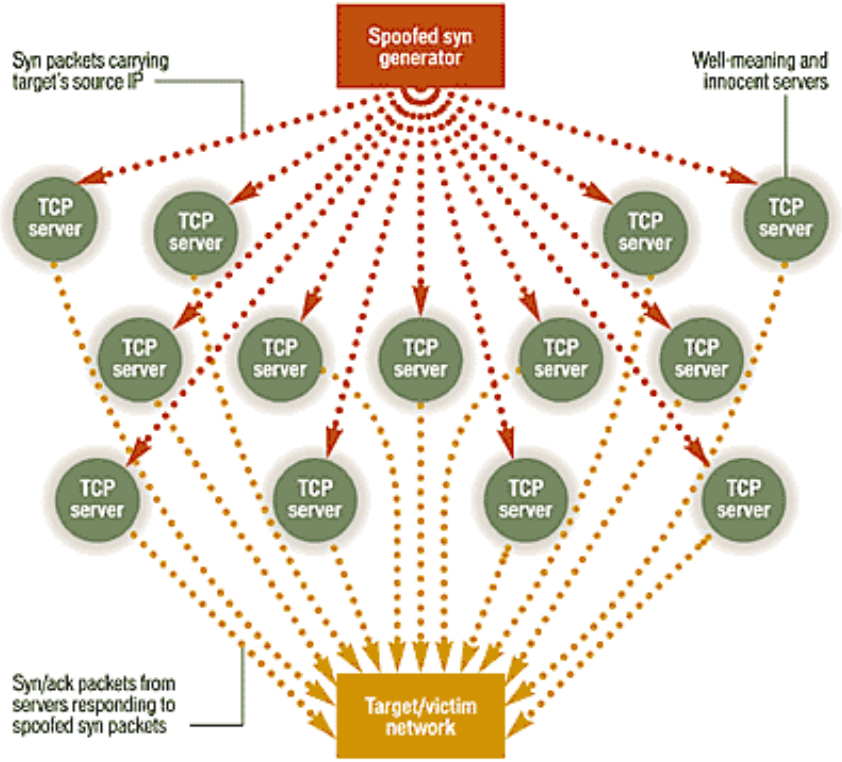
Tấn công từ chối dịch vụ

- Kỹ thuật tấn công DoS – Làm lụt bằng SYN



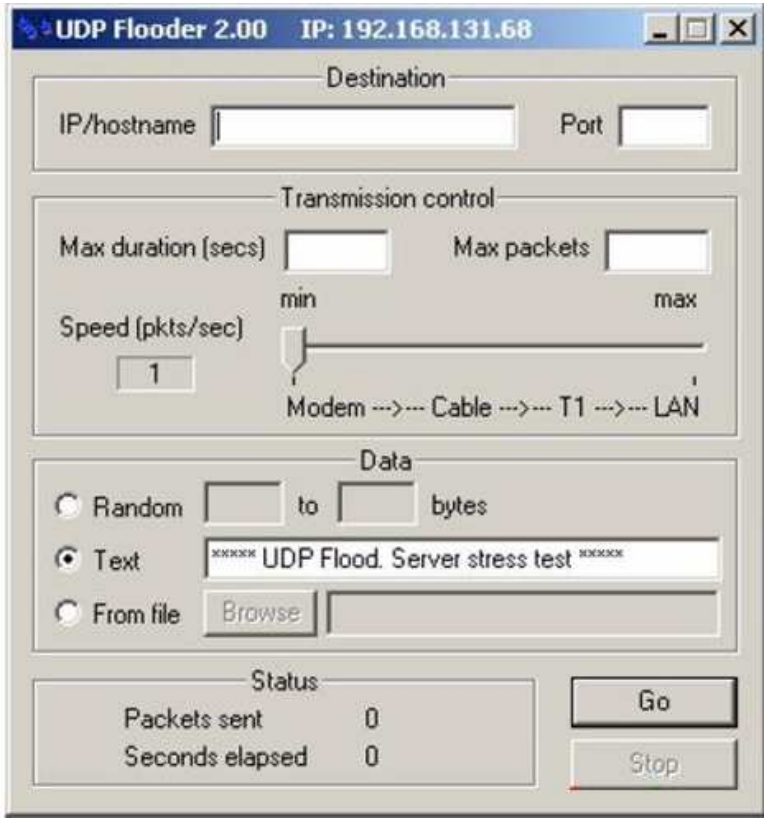
Khi Server nhận 1 yêu cầu nối kết SYN, nó sẽ trả lời lại bằng SYN/ACK và dành ra 1 khoản tài nguyên (bộ nhớ, CPU) để phục vụ cho nối kết đó và chờ tín hiệu xác nhận lại từ Client.

Nếu nhận được số nối kết vô cùng lớn, Server sẽ bị cạn kiệt tài nguyên.



Tấn công từ chối dịch vụ

- Kỹ thuật tấn công DoS



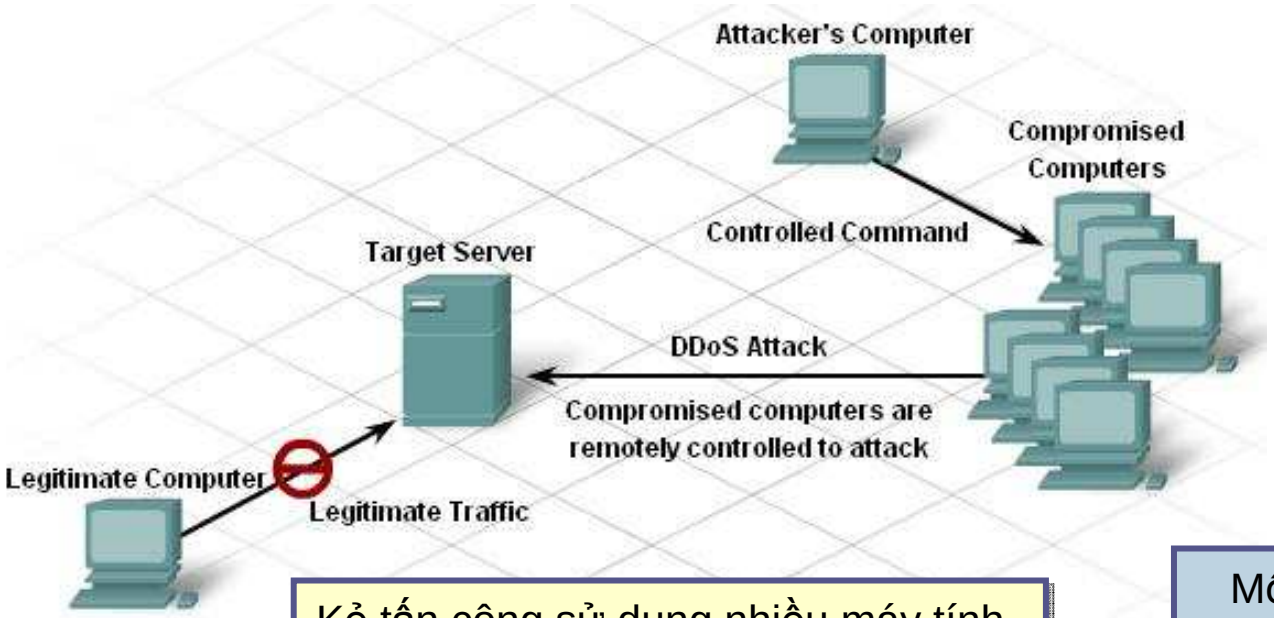
Làm lụt bằng UDP
Hacker gửi gói tin UDP echo với địa chỉ IP nguồn là cổng loopback của chính mục tiêu cần tấn công hoặc của một máy tính trong cùng mạng.

Làm lụt bằng cách dịch vụ mạng khác
- Làm quá tải Web Server bằng nhiều kết nối với cùng 1 URL.
- Gửi nhiều email đến 1 tài khoản mail.

Một số công cụ DoS thông dụng là: Jolt2, Targa, Bubonic.c, …

Tấn công từ chối dịch vụ

- Kỹ thuật tấn công DoS phân tán (DDoS)



Các máy tính bị khống chế để phục vụ tấn công DDoS gọi là **botnet**.

Kẻ tấn công sử dụng nhiều máy tính (đã chiếm quyền điều khiển) cùng 1 lúc tấn công vào 1 máy tính khác.

Một số công cụ DDoS thông dụng là: Trinoo, Stacheldraht, TFN2K, Mstream…