Tấn công mạng máy tính

- Port scan attack
- Eavesdropping attack
- IP spoofing attack
- Man-in-the-middle Attack
- Replay attack
- Hijacking Attack
- Denial of Service / Distributed Denial of Service (DoS/DDoS) Attacks
- Các loại tấn công phần mềm

Nguyên tắc truyền thông tin

- Cấu tạo gói tin TCP
- Phần giữa IP và ứng dụng

+	Bít 0 - 3	4 - 9	10 - 15	16 - 31
0	Source Port			Destination Port
32	Sequence Number			
64	Acknowledgement Number			
96	Data Offset	Reserved	Flags	Window
128	Checksum			Urgent Pointer
160	Options (optional)			
160/192+	Data			

Nguyên tắc truyền thông tin

- **Cấu tạo gói tin IP**

+	Bít 0 - 3	4 - 7	8 - 9	10 - 15	16 - 31
0	Source address				
32	Destination address				
64	Zeros		Protocol		TCP length
96	Source Port				Destination Port
128	Sequence Number				
160	Acknowledgement Number				
192	Data Offset	Reserved		Flags	Window
225	Checksum				Urgent Pointer
257	Options (optional)				
257/289+	Data				

Nguyên tắc truyền thông tin

- Các gói tin chỉ ra địa chỉ, cổng đến từ đó hệ thống mạng sẽ định hướng chuyển gói tin
- Các gói tin chỉ ra nguồn gửi để nơi nhận có phản hồi phù hợp
- Sử dụng chỉ số thứ tự để xác định cách lắp ghép
- Sử dụng các bít cờ để xác định nội dung dữ liệu, và trạng thái điều khiển

Nguyên tắc truyền thông tin

- Các pha kết nối
  - thiết lập kết nối
  - truyền dữ liệu
  - kết thúc kết nối

Nguyên tắc truyền thông tin

- Các trạng thái kết nối
- LISTEN
- SYN-SENT
- SYN-RECEIVED
- ESTABLISHED
- FIN-WAIT-1
- FIN-WAIT-2
- CLOSE-WAIT
- CLOSING
- LAST-ACK
- TIME-WAIT
- CLOSED

Nguyên tắc truyền thông tin

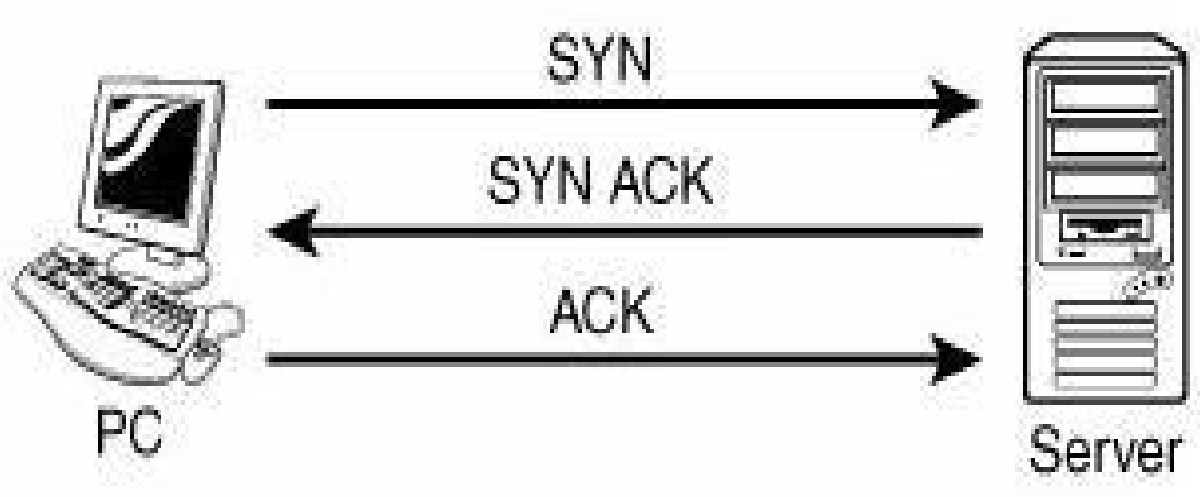
- Mô tả thông tin
  - LISTEN
    - đang đợi yêu cầu kết nối từ một TCP và cổng bất kỳ ở xa
  - SYN-SENT
    - đang đợi TCP ở xa gửi một gói tin TCP với các cờ SYN và ACK được bật
  - SYN-RECEIVED
    - đang đợi TCP ở xa gửi lại một tin báo nhận sau khi đã gửi cho TCP ở xa đó một tin báo nhận kết nối

Nguyên tắc truyền thông tin

- Mô tả thông tin
  - ESTABLISHED
    - cổng đã sẵn sàng nhận/gửi dữ liệu với TCP ở xa (đặt bởi TCP client và server)
  - TIME-WAIT
    - đang đợi qua đủ thời gian để chắc chắn là TCP ở xa đã nhận được tin báo nhận về yêu cầu kết thúc kết nối của nó. Theo RFC 793, một kết nối có thể ở tại trạng thái TIME-WAIT trong vòng tối đa 4 phút.

Kết nối

- Client: gửi gói tin SYN, tham số **sequence number** được gán cho một giá trị ngẫu nhiên **X**.
- Server: gửi lại SYN-ACK, tham số **acknowledgment number** X + 1, tham số **sequence number** được gán ngẫu nhiên **Y**
- Client: gửi ACK, tham số **sequence number** X + 1,tham số **acknowledgment number** Y + 1



Kết thúc phiên

- + Bước I: Client gửi đến FIN ACK
  + Bước II: Server gửi lại c ACK
  + Bước III: Server lại gửi FIN ACK
  + Bước IV: Client gửi lại ACK

Gói tin UDP

- Cấu trúc UDP

offset (bits)	0 – 15	16 – 31
0	Source Port Number	Destination Port Number
32	Length	Checksum
64+	Data	

Gói tin UDP

- IPv4 UDP

bits	0 – 7	8 – 15	16 – 23	24 – 31
0	Source address			
32	Destination address			
64	Zeros	Protocol	UDP length	
96	Source Port		Destination Port	
128	Length		Checksum	
160+	Data			

Nguyên tắc Port scan

- 1. TCP Scan
- Trên gói TCP/UDP có 16 bit dành cho Port Number điều đó có nghĩa nó có từ 1 – 65535 port.
- Thường chỉ scan từ 1 - 1024.
- Một số phương pháp:

Nguyên tắc Port scan

- SYN Scan:
  - Gửi SYN với một thông số Port
  - Nhận SYN/ACK thì Client biết Port đó trên Server được mở.
  - Ngược lại Client nhận gói RST/SYN.
- FIN Scan:
  - Client gửi gói FIN với số port nhất định.
  - Nhận ACK thì Server mở port đó,
  - Server gửi về gói RST thì Client biết Server đóng port đó.

Nguyên tắc Port scan

- NULL Scan Sure:
  - Client gửi tới Server những gói TCP với số port cần Scan không chứa thông số Flag nào,
  - Server gửi lại gói RST thì tôi biết port đó trên Server bị đóng.
- XMAS Scan Sorry:
  - Client gửi gói TCP với số Port nhất định cần Scan chứa nhiều Flag như: FIN, URG, PSH.
  - Nếu Server trả về gói RST tôi biết port đó trên Server bị đóng.

Nguyên tắc Port scan

- **TCP Connect:**
  - gửi đến Server những gói tin yêu cầu kết nối port cụ thể trên server.
  - Nếu server trả về gói SYN/ACK thì mở cổng đó.
- **ACK Scan:**
  - Scan này nhằm mục đích tìm những Access Controll List trên Server. Client cố gắng kết nối tới Server bằng gói ICMP
  - nhận được gói tin là Host Unreachable thì client sẽ hiểu port đó trên server đã bị lọc.

Công cụ portscan

- Tự xây dựng dựa trên cấu mô tả
- RPC Scan: Kiểm tra dịch vụ RPC
- Windows Scan: tương tự như ACK Scan, nhưng nó có thể chỉ thực hiện trên một số port nhất định.
- FTP Scan: Có thể sử dụng để xem dịch vụ FTP có được sử dụng trên Server hay không
- IDLE: cho phép kiểm tra tình trạng của máy chủ.

Eavesdropping attack

- Nghe lén
- Mục tiêu: thu nhận thông tin truyền
  - Nhận được các thông tin truyền không mã hóa
  - Nhận được các thông tin đã mã hóa, từ đó phục vụ các tấn công khác (replay attack)
- Không để dấu vết
- Khó phòng chống

Eavesdropping attack

- Sử dụng các phương pháp vật lý
  - Nghe trộm qua đường truyền vật lý
  - Qua hệ thống sống vô tuyến
- Nghe lén mạng
  - Tham gia vào mạng
  - Nhận các gói tin được truyền đến cổng mạng
  - Nếu mạng sử dụng là switch thì cần phải sử dụng phương pháp man – in – the - middle
- Nghe lén bằng phần mềm gián điệp

Eavesdropping attack

- Ettercap, Ethereal, dsniff, TCPdump, Sniffit,...
- Nhiều công cụ phần cứng khác tham gia vào các mạng, phương thức truyền

Eavesdropping attack

- Một số phương pháp phòng chống:
- Sử dụng switch thay cho hub
- Giám sát địa chỉ MAC
- Sử dụng cơ chế mã hóa truyền tin, và mã hóa theo thời gian

Eavesdropping attack

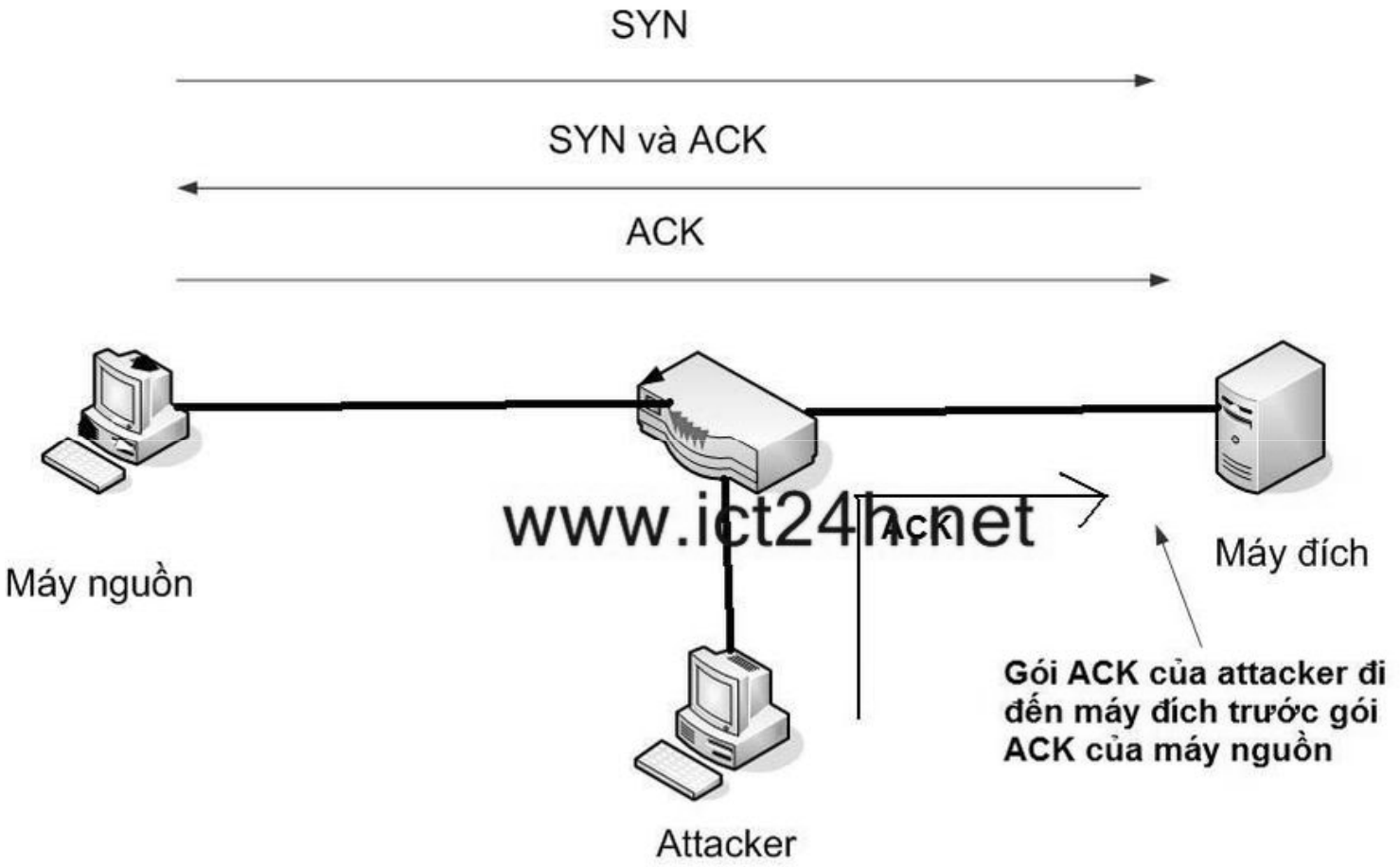
- Sử dụng các dịch vụ mã hóa trong liên kết: SSL (Secure Sockets Layer), thiết lập IPSec và mạng riêng ảo VNP (Virtual Private Network),... sử dụng SSH (Secure Shell Host) thay cho Telnet, Rlogin; dùng SFTP (secure FTP) thay vì FTP; dùng giao thức https thay cho http v.v…

Eavesdropping attack

- Sử dụng các phần mềm phát hiện sự hoạt động của các chương trình nghe lén trên mạng như AntiSniff, PromiScan, Promqry and PromqryUI, ARPwatch, Ettercap, v.v… Riêng với Ettercap (http://ettercap.sourceforge.net),
- Các công cụ chống tấn công gián điệp

Eavesdropping attack

- Tạo ra các gói tin có địa chỉ IP giả mạo không là địa chỉ máy gửi gói tin
- Vượt qua các kiểm soát về nguồn gốc địa chỉ ip
- Phục vụ các mô hình tấn công khác
  - Tấn công về phiên
  - Tấn công kiểu phản xạ
- Giải pháp
  - Không sử dụng xác thực là địa chỉ IP
  - Phát hiện các bất thường về kết nối mạng

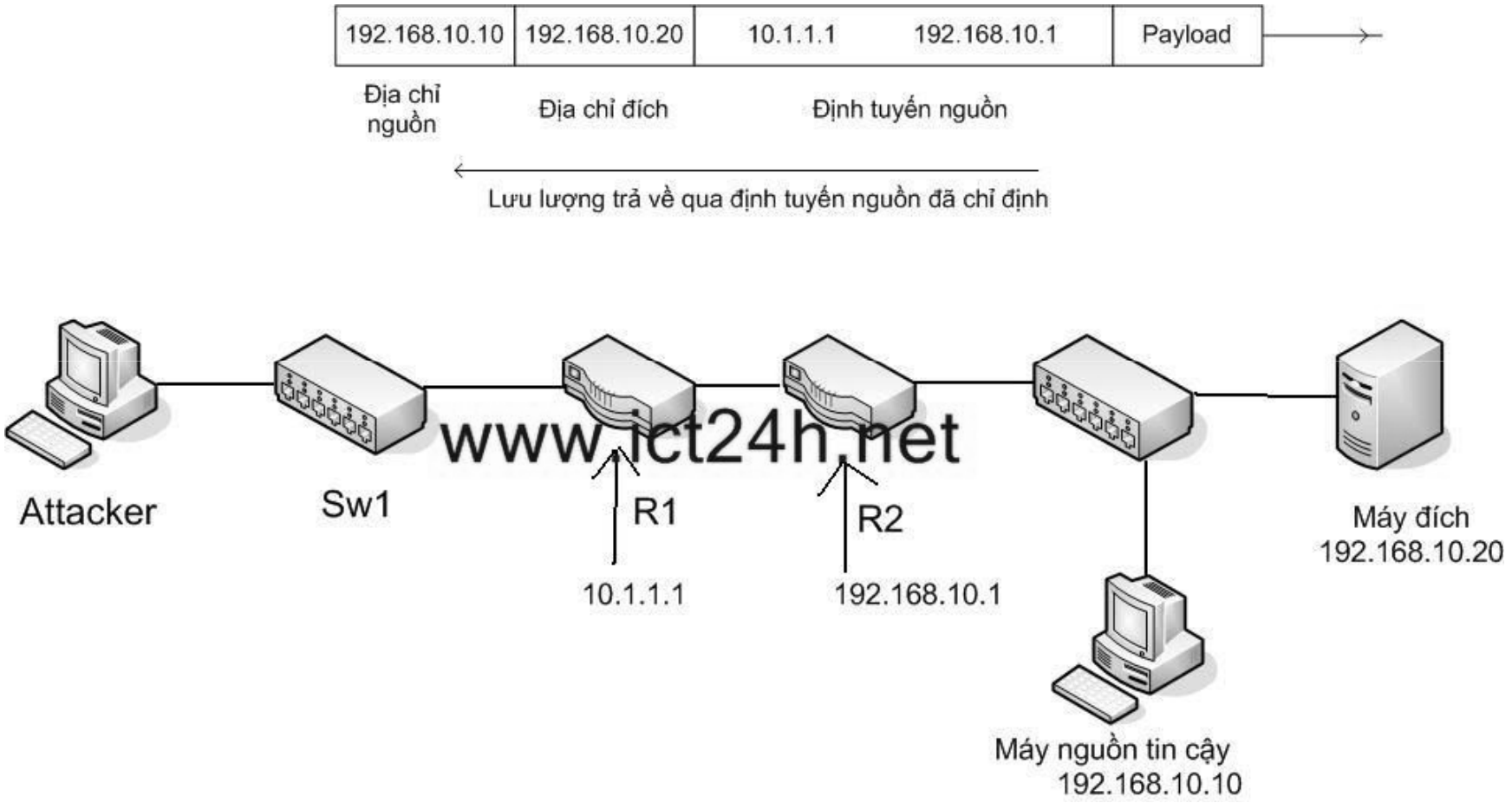


TCP spoofing

- Ta có 2 loại giả mạo địa chỉ IP:
- Giả mạo bằng cách bắt gói (non-blind spoofing), phân tích số thứ tự, cho máy cùng mạng.
- Giả mạo địa chỉ IP từ xa (blind spoofing): khác mạng, có được số TCP sequence chính xác là rất khó.Tuy nhiên , với một số kĩ thuật, chẳng hạn như định tuyến theo địa chỉ nguồn,máy tấn công cũng có thể xác định chính xác được chỉ số đó.

ĐỊNH TUYẾN THEO NGUỒN

- IP source routing là một cơ chế cho phép một máy nguồn chỉ ra đường đi một cách cụ thể và không phụ thuộc vào bảng định tuyến của các router.
- Kẻ tấn công gửi gói tin và đưa ra bảng định tuyến theo đường cố định. Nơi nhận gói tin theo đúng bảng đinht uyến có sẵn gửi lại.


192.168.10.10
192.168.10.20
10.1.1.1
192.168.10.1
Payload
Địa chỉ nguồn
Địa chỉ đích
Định tuyến nguồn
Lưu lượng trả về qua định tuyến nguồn đã chỉ định
www.ict24h.net
Attacker
Sw1
R1
R2
10.1.1.1
192.168.10.1
Máy đích
192.168.10.20
Máy nguồn tin cậy
192.168.10.10

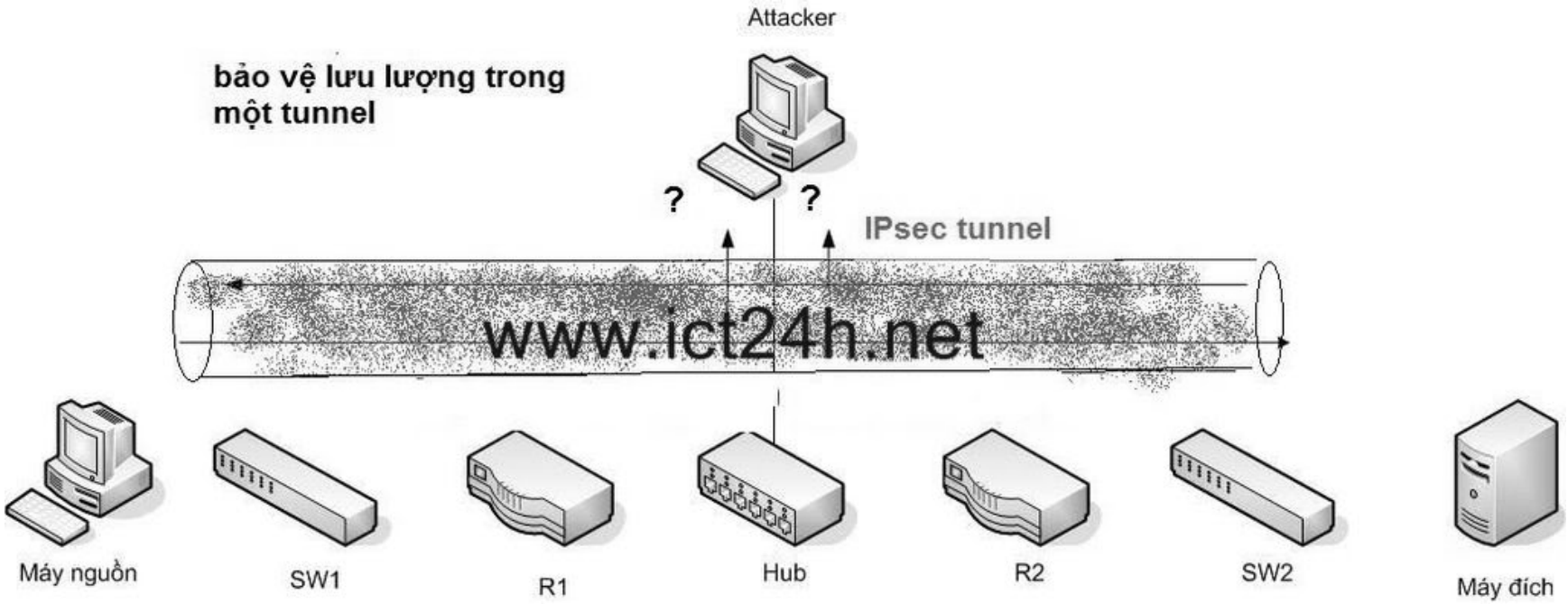
CHỐNG GIẢ MẠO ĐỊA CHỈ IP

- Để làm giảm nguy cơ tấn công giả mạo địa chỉ IP cho một hệ thống mạng,ta có thể sử dụng các phương pháp sau:
  -Dùng danh sách kiểm tra truy cập (Access Control List-ACL) trên các interface của router. Một ACL có thể dc dùng để loại bỏ những traffic từ bên ngoài mà lại được đóng gói bởi một địa chỉ trong mạng cục bộ khi bị lôi cuốn vào một cuộc tấn công Ddos.

-

CHỐNG GIẢ MẠO ĐỊA CHỈ IP

- Dùng mật mã xác thực.Nếu cả hai đầu của cuộc nói chuyện đã được xác thực, khả năng tấn công theo kiểu Man-in-the-middle có thể được ngăn cản.
  -Mã hoá traffic giữa các thiết bị (giữa 2 router,hoặc giữa 2 hệ thống cuối và router) bằng một IPSec tunnel


bảo vệ lưu lượng trong một tunnel
Attacker
?
?
IPsec tunnel
www.ict24h.net
Máy nguồn
SW1
R1
Hub
R2
SW2
Máy đích

Kết luận

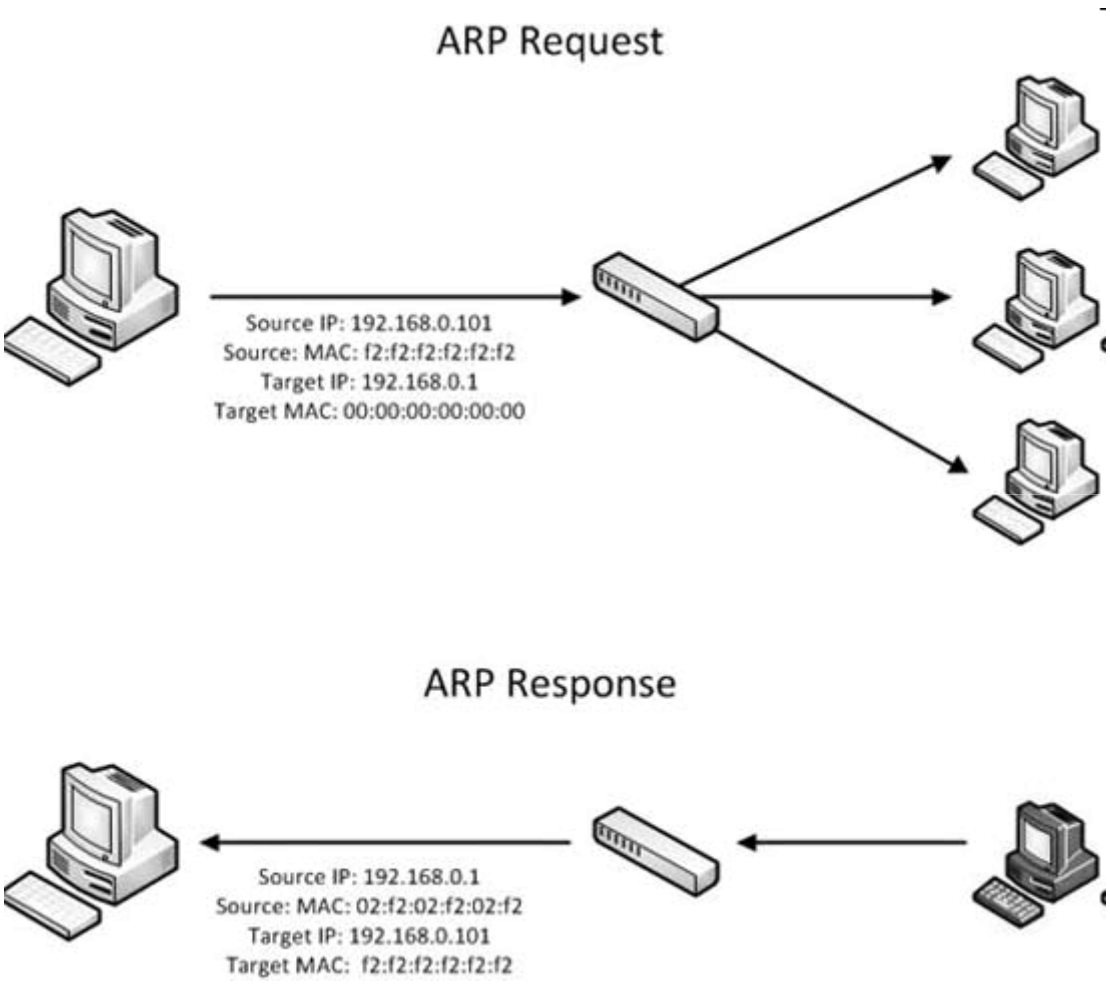
- IP giả mạo là một vấn đề khó khăn để giải quyết, bởi vì nó liên quan đến cấu trúc gói tin IP.
- Mặc dù không có giải pháp dễ dàng cho các vấn đề giả mạo IP, bạn có thể áp dụng một số phương pháp chủ động và phản ứng đơn giản tại các nút, và sử dụng các bộ định tuyến trong mạng để giúp phát hiện một gói tin giả mạo và theo dõi nó trở lại với nguồn có nguồn gốc của nó.

Man-in-the-middle Attack

1.Khái niệm

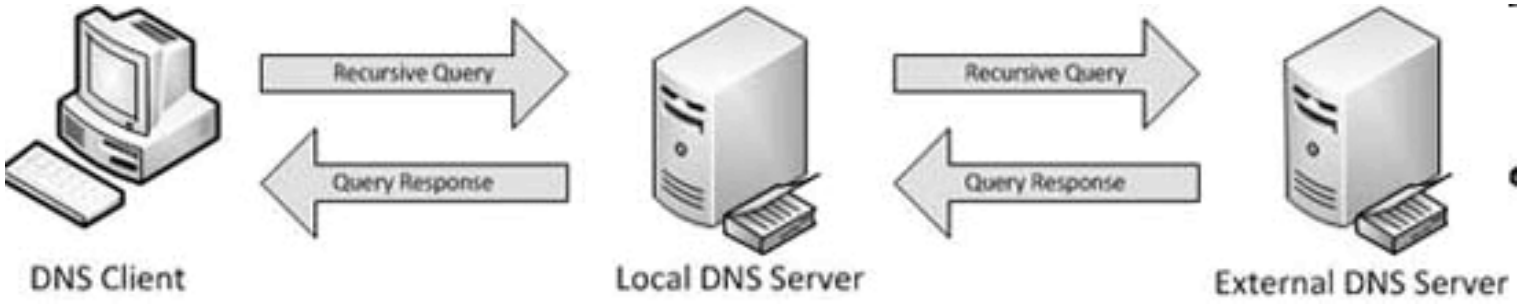
- Tấn công khi làm cho hai bên kết nối, hiểu nhầm người thứ 3 là đối tác của mình
- Tấn công bằng bộ phát sống giả mạo (AP)
  - Sử dụng bộ phát có sóng mạnh hơn
  - Máy kết nối nhầm, hoặc xác thực nhầm
- Tấn công bằng làm giả tín hiệu tính hiệu ARP
  - Gửi các thông điệp map giữa IP và MAC

1.Khái niệm


ARP Request
Source IP: 192.168.0.101
Source: MAC: f2:f2:f2:f2:f2:f2
Target IP: 192.168.0.1
Target MAC: 00:00:00:00:00:00
ARP Response
Source IP: 192.168.0.1
Source: MAC: 02:f2:02:f2:02:f2
Target IP: 192.168.0.101
Target MAC: f2:f2:f2:f2:f2:f2

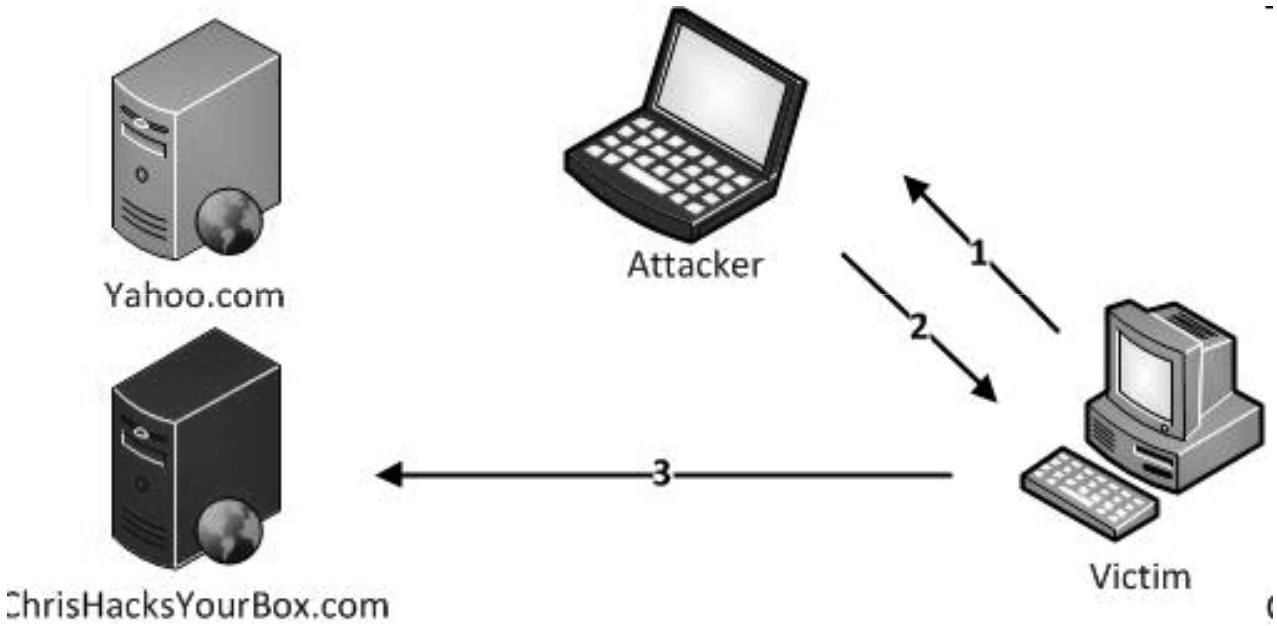
1.Khái niệm

- Tấn công vào DNS
  - Dựa trên cơ chế gửi và nhận địa chỉ IP thông qua tên miền
  - Gửi một địa chỉ IP khác với địa chỉ tên miền



1.Khái niệm

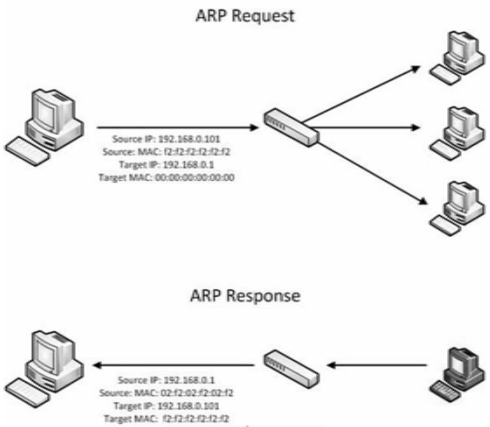
- Tấn công vào DNS



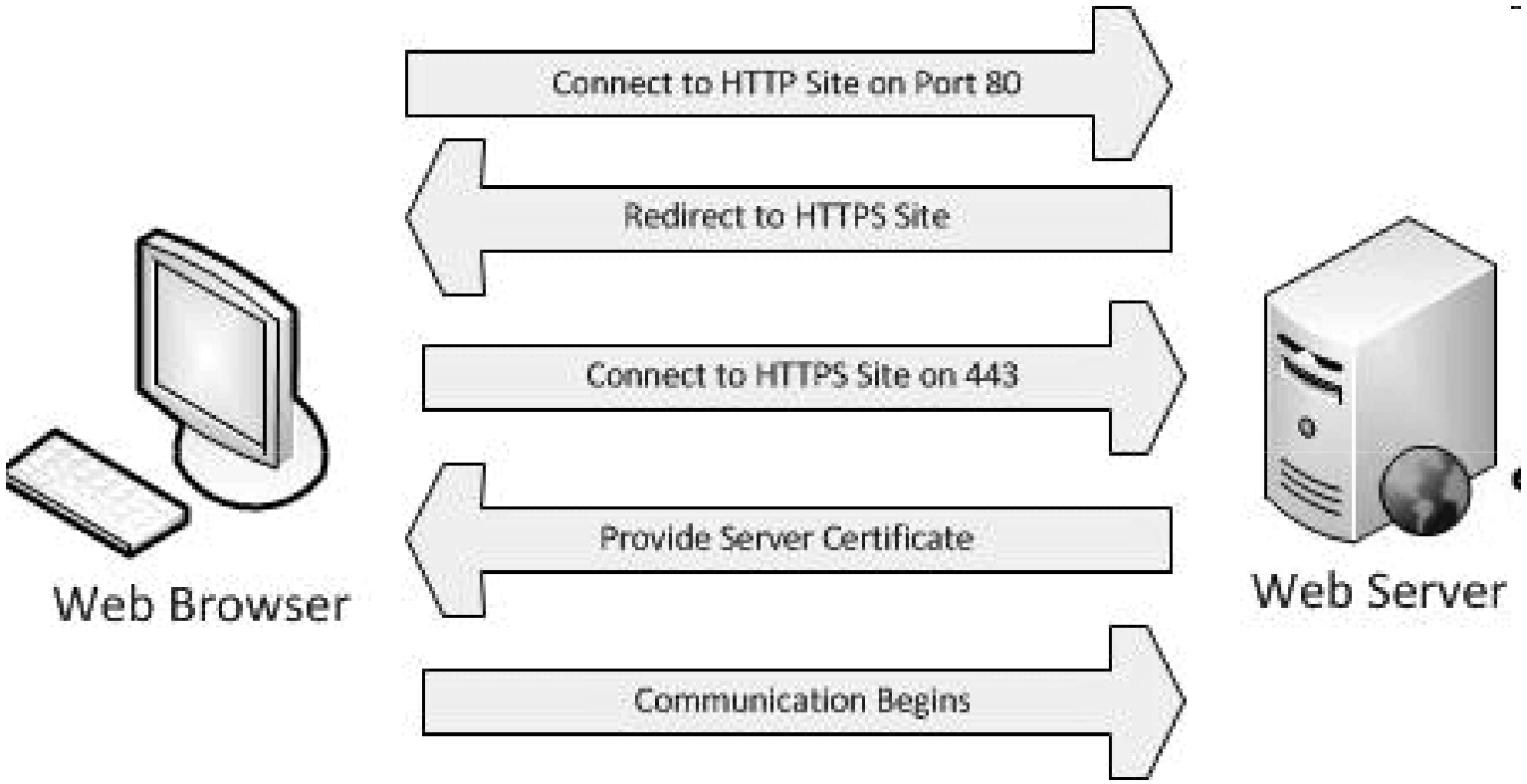
1. Legitimate DNS Request Destined for DNS Server
2. Fake DNS Reply from Listening Attacker
3. Victim begins communicating with malicious site as a result

a. Phương thức tân công giả mạo ARP Cache

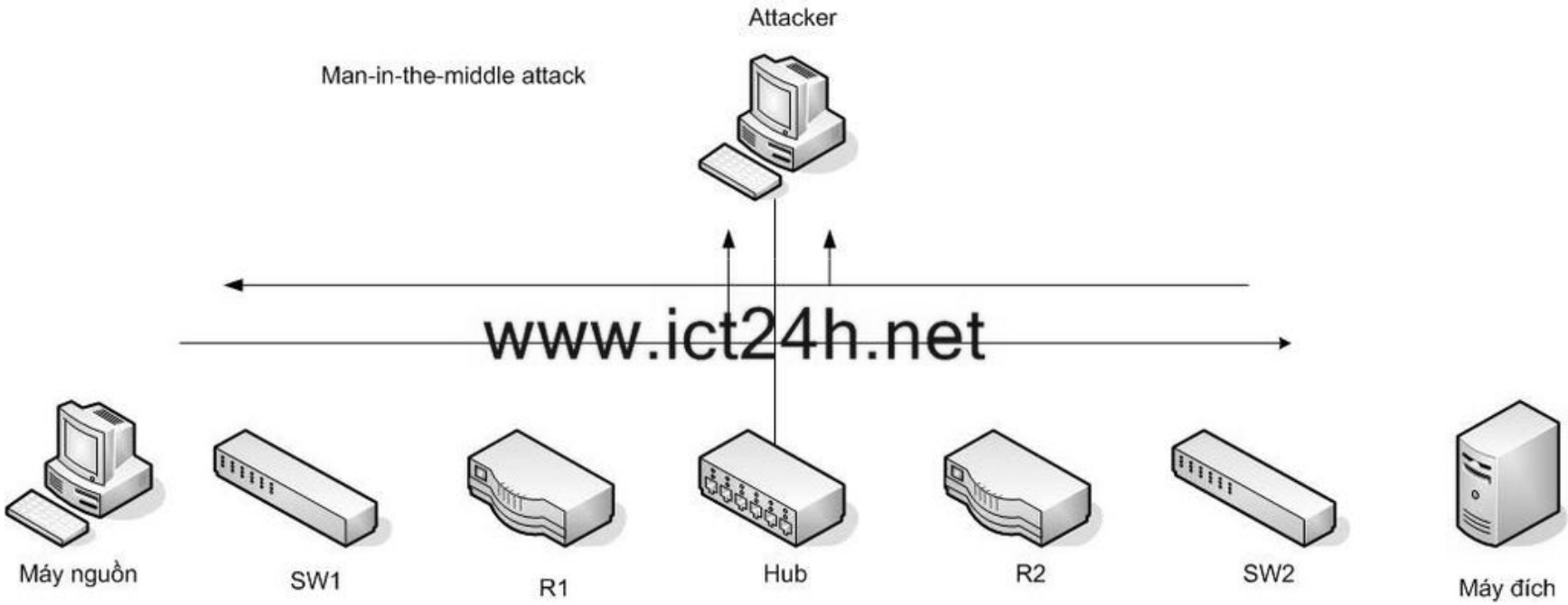
- a.1 Giả mạo ARP Cache (ARP Cache Poisoning): Làm trung gian quá trình truyền tin.
- a.2 Truyền thông AR. Giao thức ARP được thiết kế để phục vụ cho nhu cầu thông dịch các địa chỉ giữa các lớp thứ hai và thứ ba của mô hình OSI.
- //Lớp thứ hai (lớp data-link) sử dụng địa chỉ MAC để các thiết bị phần cứng có thể truyền thông với nhau một cách trực tiếp.



Quá trình truyền thông ARP


Connect to HTTP Site on Port 80
Redirect to HTTPS Site
Connect to HTTPS Site on 443
Provide Server Certificate
Communication Begins
Web Browser
Web Server

- Giả mạo AP, ARP đưa ra trang web trung gian để giả các giao thức SSL, ...


Attacker
Man-in-the-middle attack
www.ict24h.net
Máy nguồn
SW1
R1
Hub
R2
SW2
Máy đích

4. Công cụ MITM tấn công

- Có một số công cụ để nhận ra một cuộc tấn công MITM. Những công cụ này đặc biệt hiệu quả trong môi trường mạng LAN, bởi vì họ thực hiện các chức năng thêm, như khả năng giả mạo arp cho phép đánh chặn của giao tiếp giữa các máy.
- PacketCreator
- Ettercap
- Dsniff
- Cain e Abel

5. Cách chống lại tấn công MITM

- Bảo mật vật lý (Physical security) là phương pháp tốt nhất để chống lại kiểu tấn công này.
- Ngoài ra, ta có thể ngăn chặn hình thức tấn công này bằng kỹ thuật mã hoá: mã hoá traffic trong một đường hầm IPSec, hacker sẽ chỉ nhìn thấy những thông tin không có giá trị.

6. hình thức tấn công MITM:

- - Giả mạo ARP Cache
- - Chiếm quyền điểu khiển SSL
- - DNS Spoofing

Replay attack
(tấn công phát lại)

Thẻ phiên

- Sử dụng thông tin nghe lén
  - Lưu trữ
  - Gửi lại thông tin đến máy cần để xác thực
- Giải pháp
  - Xác thực theo phiên (chỉ số phiên)
  - Sử dụng phương pháp xác thực lại theo thời gian (sau thời gian kết nối)

Mô hình

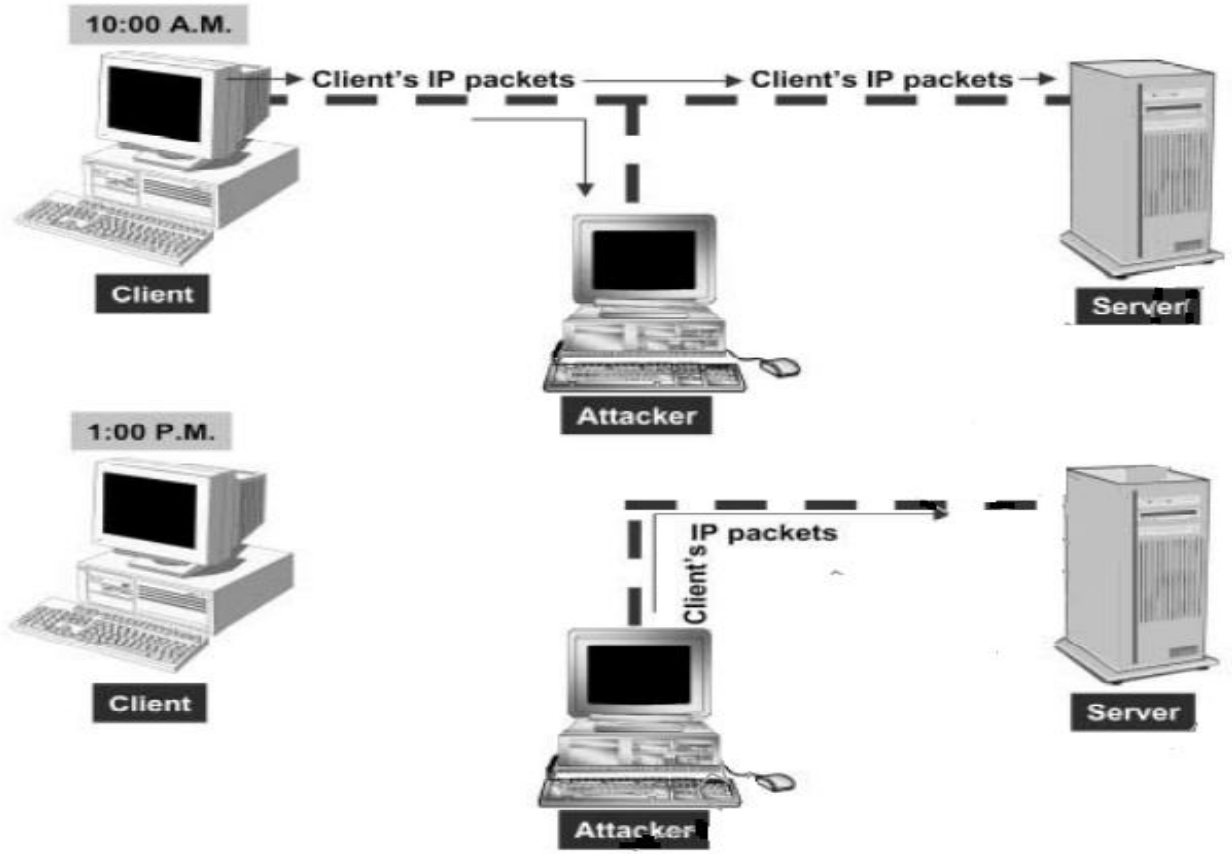
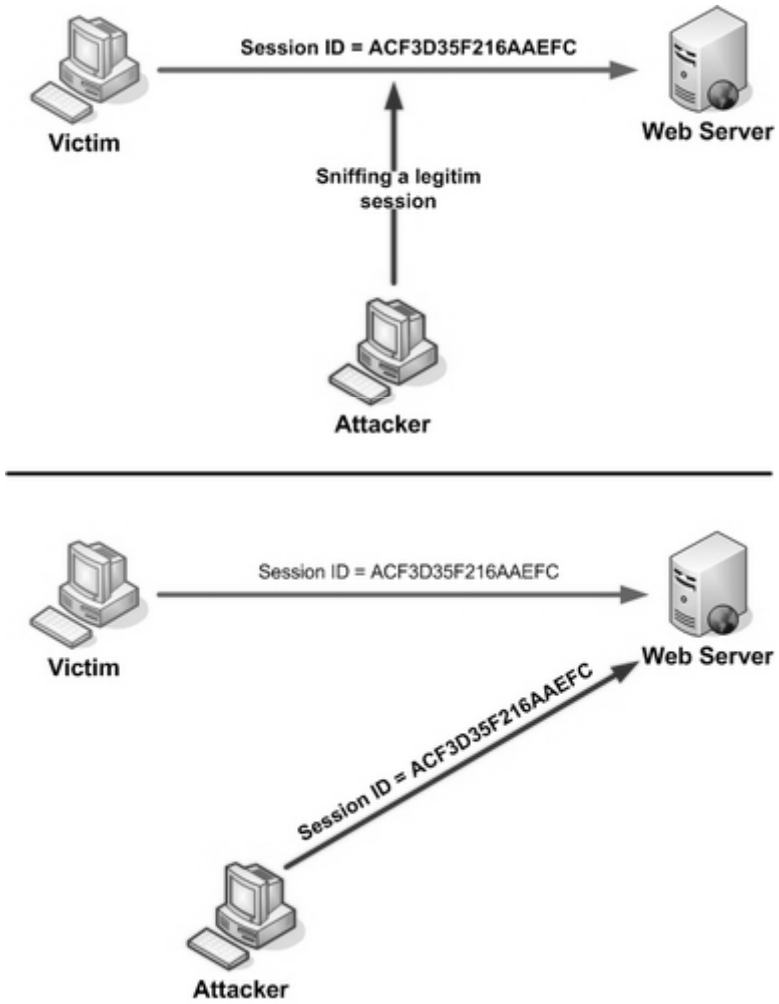


Figure 1-6: *Replay attacks.*

HIJACKING ATTACK
Kẻ tấn công chiếm quyền điều khiển

- Nghe lén trao đổi
- Gửi tín hiệu cắt kết nối client
- Tiếp tục kết nối với server

HIJACKING ATTACK



I. Thế nào là một kẻ tấn công chiếm quyền điều khiển?

- Nghe lén thông tin liên lạc
- Đợi kết thúc quá trình xác thực
- Gửi tín hiệu yêu cầu kết thúc
- Tiếp tục liên kết với máy còn lại

II. Giải pháp

- Tiến hành mã hóa phiên
- Xác thực phiên theo thời gian

V. Công cụ kẻ tân công chiêm quyền điều khiển sử dụng:

- Có một vài chương trình có sẵn có thể thực hiện được việc chiếm quyền điều khiển.
- Dưới đây là một vài chương trình thuộc loại này:
  - Juggernaut
  - Hunt
  - IP Watcher
  - T-Sight
  - Paros HTTP Hijacker


Certified e-Business Professional

Tấn công từ chối dịch vụ

- Tấn công làm cho một hệ thống nào đó bị quá tải không thể cung cấp dịch vụ hoặc phải ngưng hoạt động.
- Tấn công kiểu này chỉ làm gián đoạn hoạt động của hệ thống chứ rất ít có khả năng thâm nhập hay chiếm được thông tin dữ liệu của nó

Các loại tấn công từ chối dịch vụ

- Tấn công từ chối dịch vụ cổ điển **DoS (Denial of Service)**
- Tấn công từ chối dịch vụ phân tán **DDoS (Distributed Denial of Service)**
- Tấn công từ chối dịch vụ theo phương pháp phản xạ **DRDoS (Distributed Reflection Denial of Service).**

Biến thể của tấn công DoS

- Broadcast Storms
- SYN
- Finger
- Ping
- Flooding,…

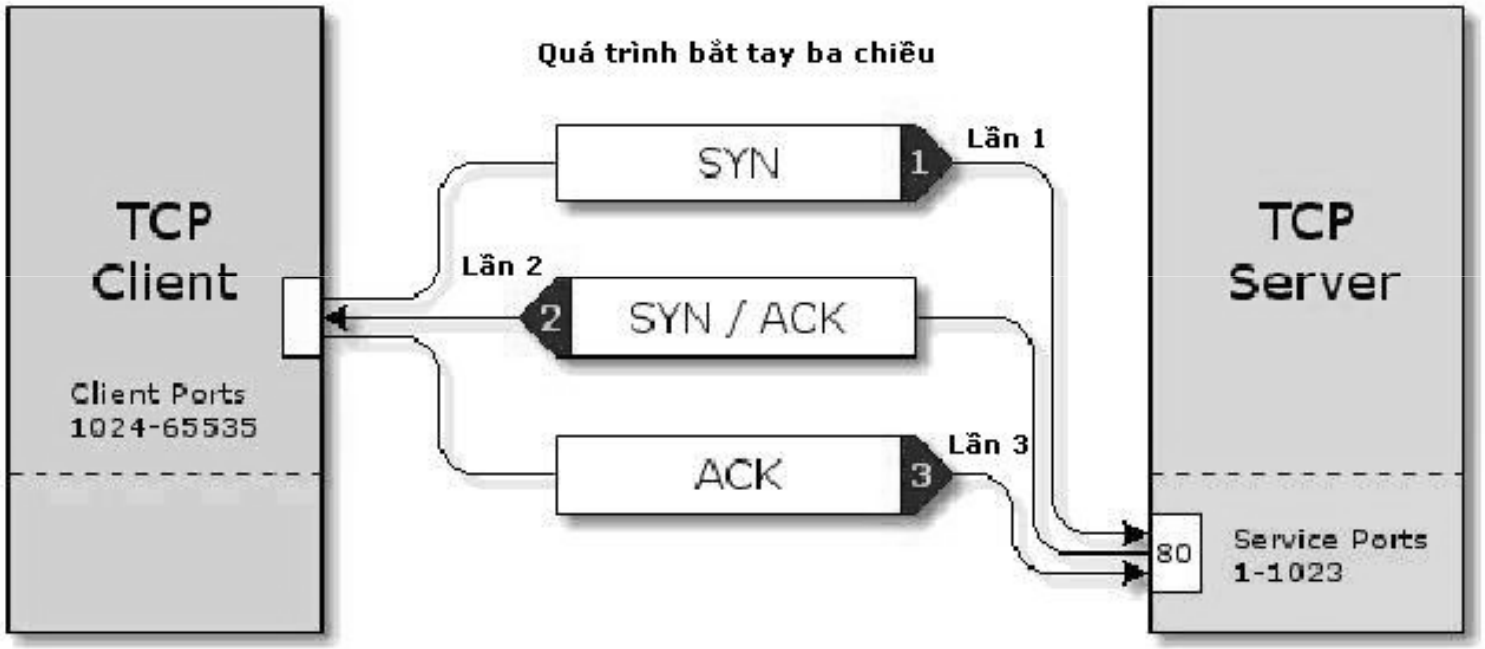
Mục tiêu tấn công DoS

- Mục tiêu nhằm chiếm dụng các tài nguyên của hệ thống (máy chủ) như: Bandwidth, Kernel Table, Swap Space, Cache, Hardisk, RAM, CPU,…
- Làm hoạt động của hệ thống bị quá tải dẫn đến không thể đáp ứng được các yêu cầu (request) hợp lệ nữa.

Tấn công từ chối dịch vụ cổ điển

- Là phương thức xuất hiện đầu tiên, giản đơn nhất trong kiểu tấn công từ chối dịch vụ.Các kiểu tấn công thuộc phương thức này rất đa dạng
- Ví dụ một dạng tấn công tiêu biểu:
  - SYN Attack

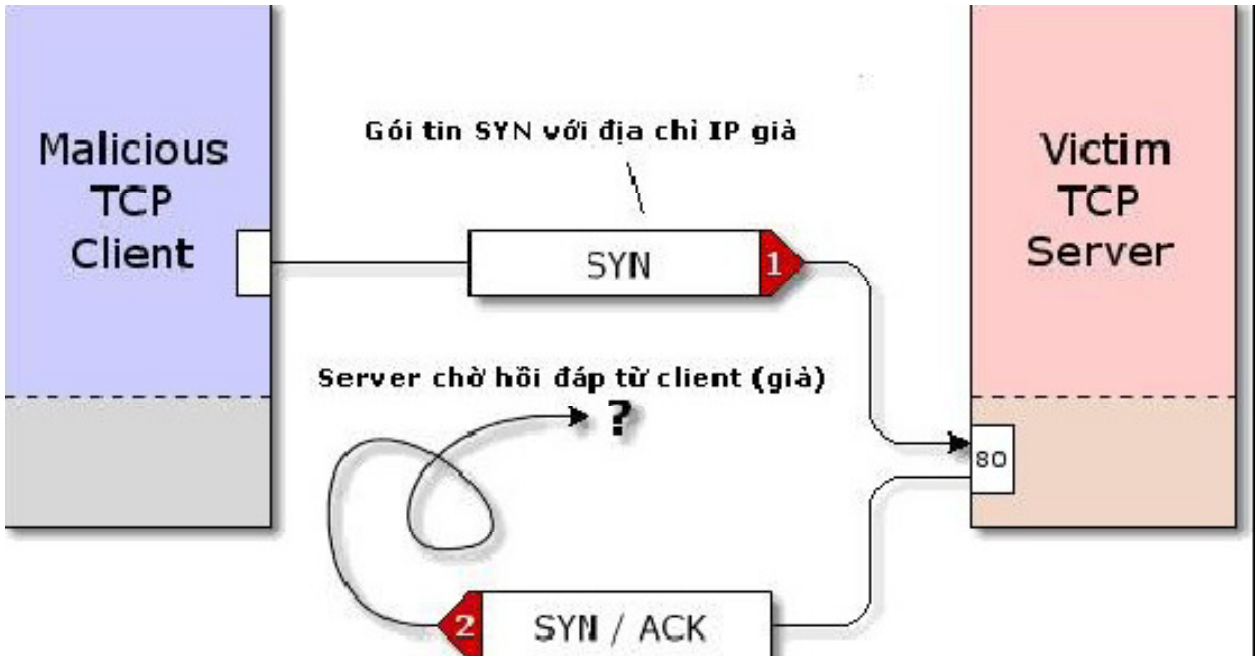
Bắt tay ba chiều trong kết nối TCP



Bắt tay ba chiều trong kết nối TCP

- Bước 1: Client (máy khách) sẽ gửi các gói tin (packet chứa SYN=1).
- Bước 2: Server sẽ gửi lại gói tin SYN/ACK, chuẩn bị tài nguyên cho việc yêu cầu này.
- Bước 3: Cuối cùng, client hoàn tất việc bắt tay ba lần bằng cách hồi âm lại gói tin chứa ACK cho server và tiến hành kết nối.

DoS dùng kỹ thuật SYN Flood



DoS dùng kỹ thuật SYN Flood

- Hacker cài một chương trình phá hoại (malicious code) vào client.
- Client không hồi đáp tín hiệu ACK (bước 3) về cho server.
- Server không còn tài nguyên phục vụ cho những yêu cầu truy cập hợp lệ.

DoS dùng kỹ thuật SYN Flood

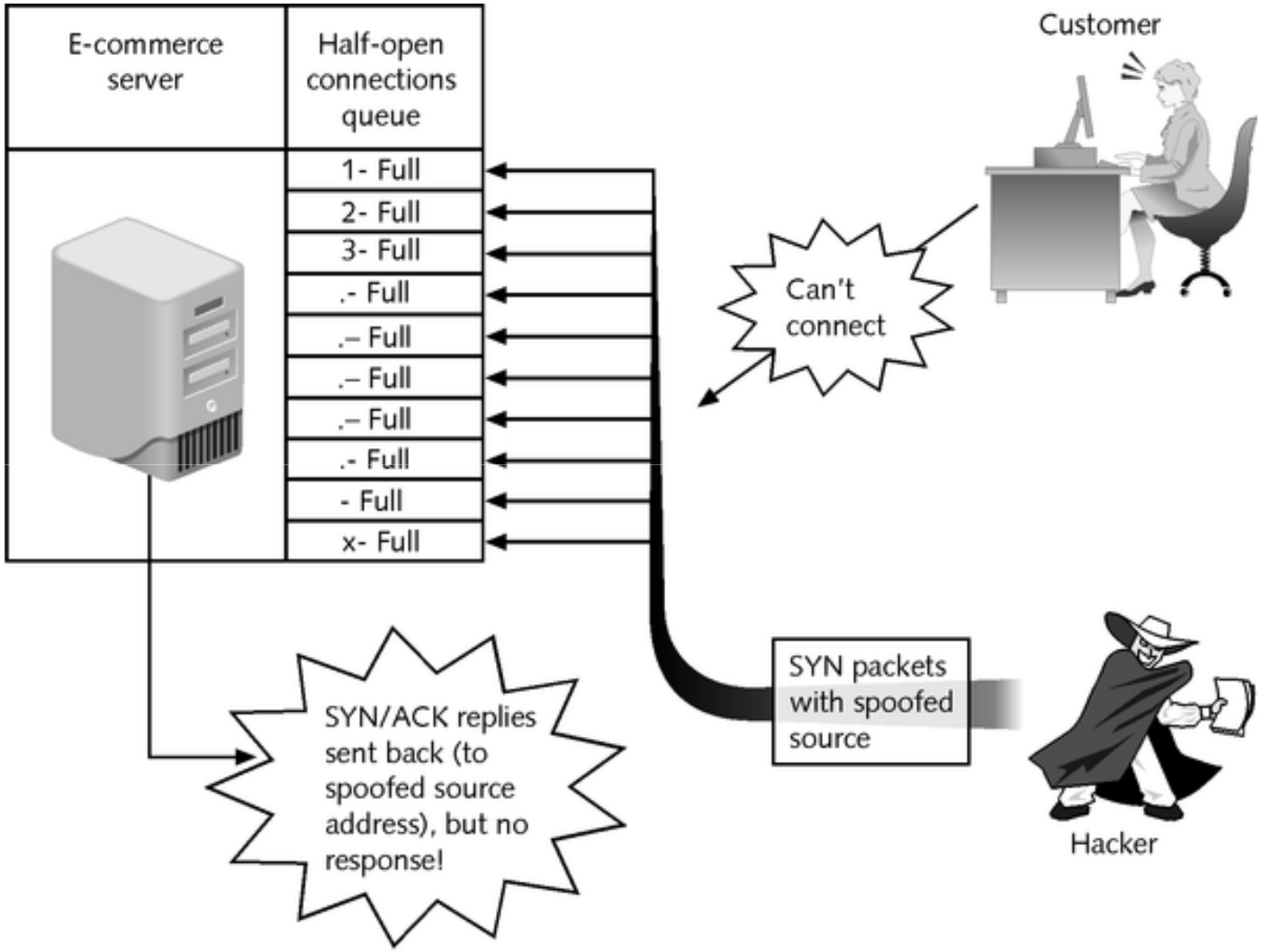
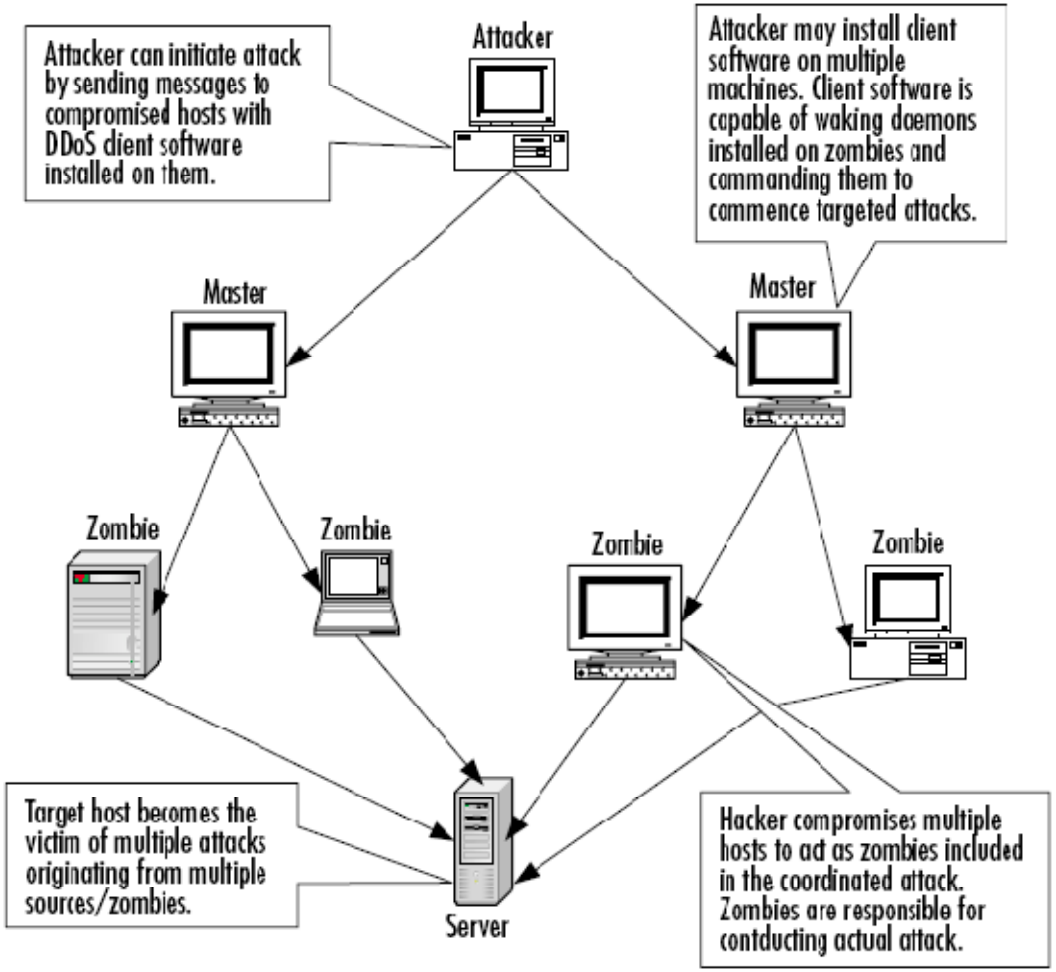


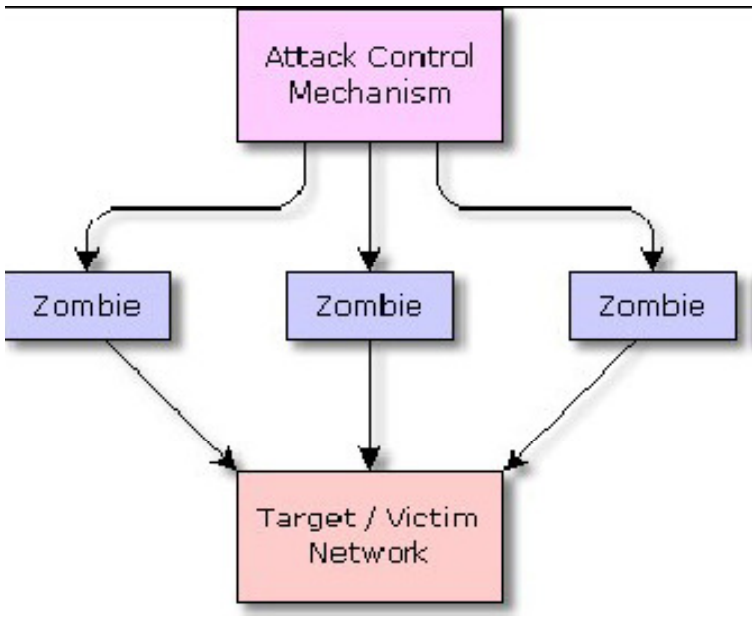
Figure 3-2 SYN flood attack

Tấn công từ chối dịch vụ kiểu phân tán (DDoS)

- Xuất hiện vào mùa thu 1999
- So với tấn công DoS cổ điển, sức mạnh của DDoS cao hơn gấp nhiều lần.
- Hầu hết các cuộc tấn công DDoS nhằm vào việc chiếm dụng băng thông (bandwidth) gây nghẽn mạch hệ thống dẫn đến hệ thống ngưng hoạt động.


Attacker can initiate attack by sending messages to compromised hosts with DDoS client software installed on them.
Attacker
Attacker may install client software on multiple machines. Client software is capable of waking daemons installed on zombies and commanding them to commence targeted attacks.
Master
Master
Zombie
Zombie
Zombie
Zombie
Target host becomes the victim of multiple attacks originating from multiple sources/zombies.
Server
Hacker compromises multiple hosts to act as zombies included in the coordinated attack. Zombies are responsible for contducting actual attack.

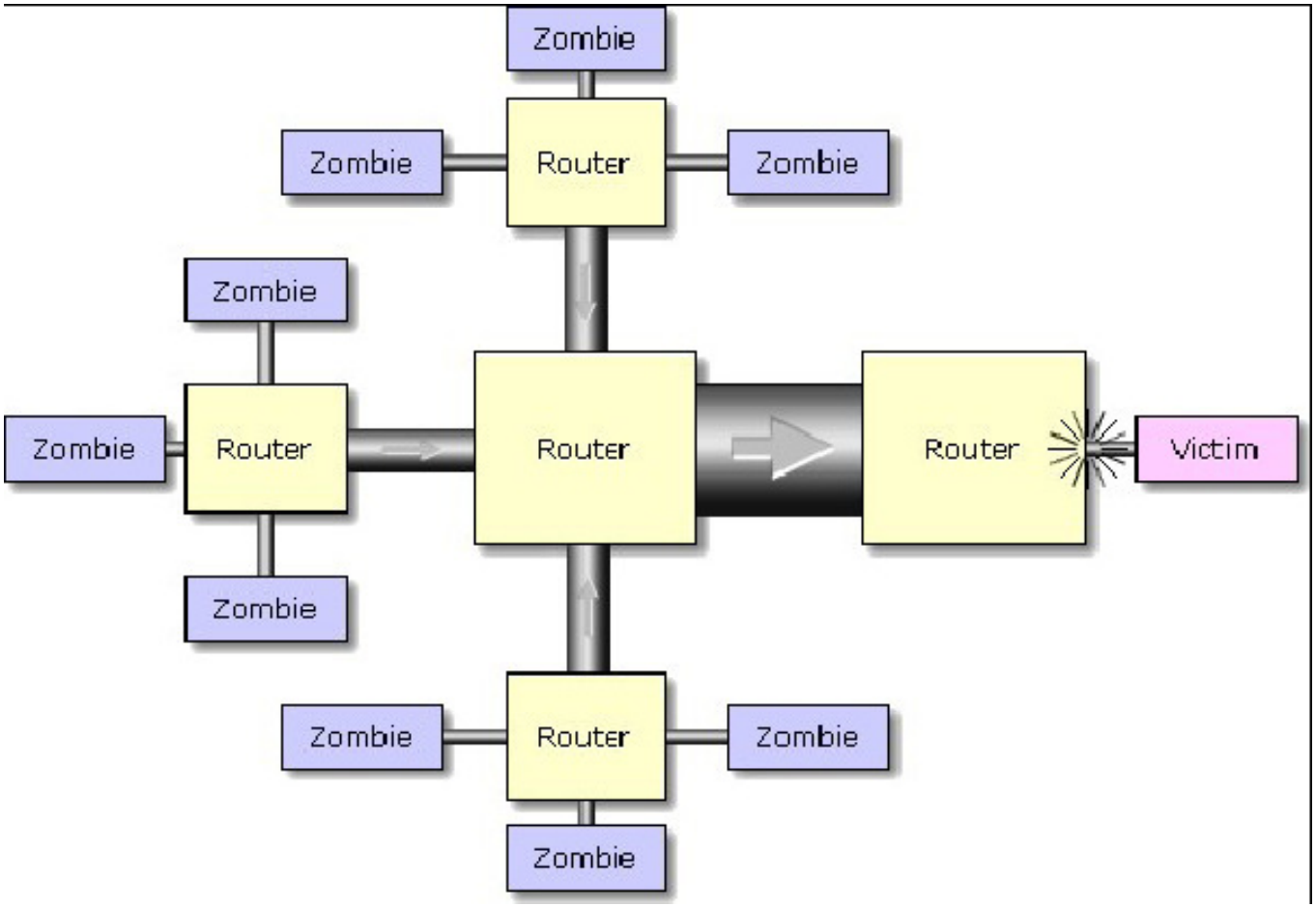
Tấn công từ chối dịch vụ kiểu phân tán (DDoS)



Tấn công từ chối dịch vụ kiểu phân tán (DDoS)

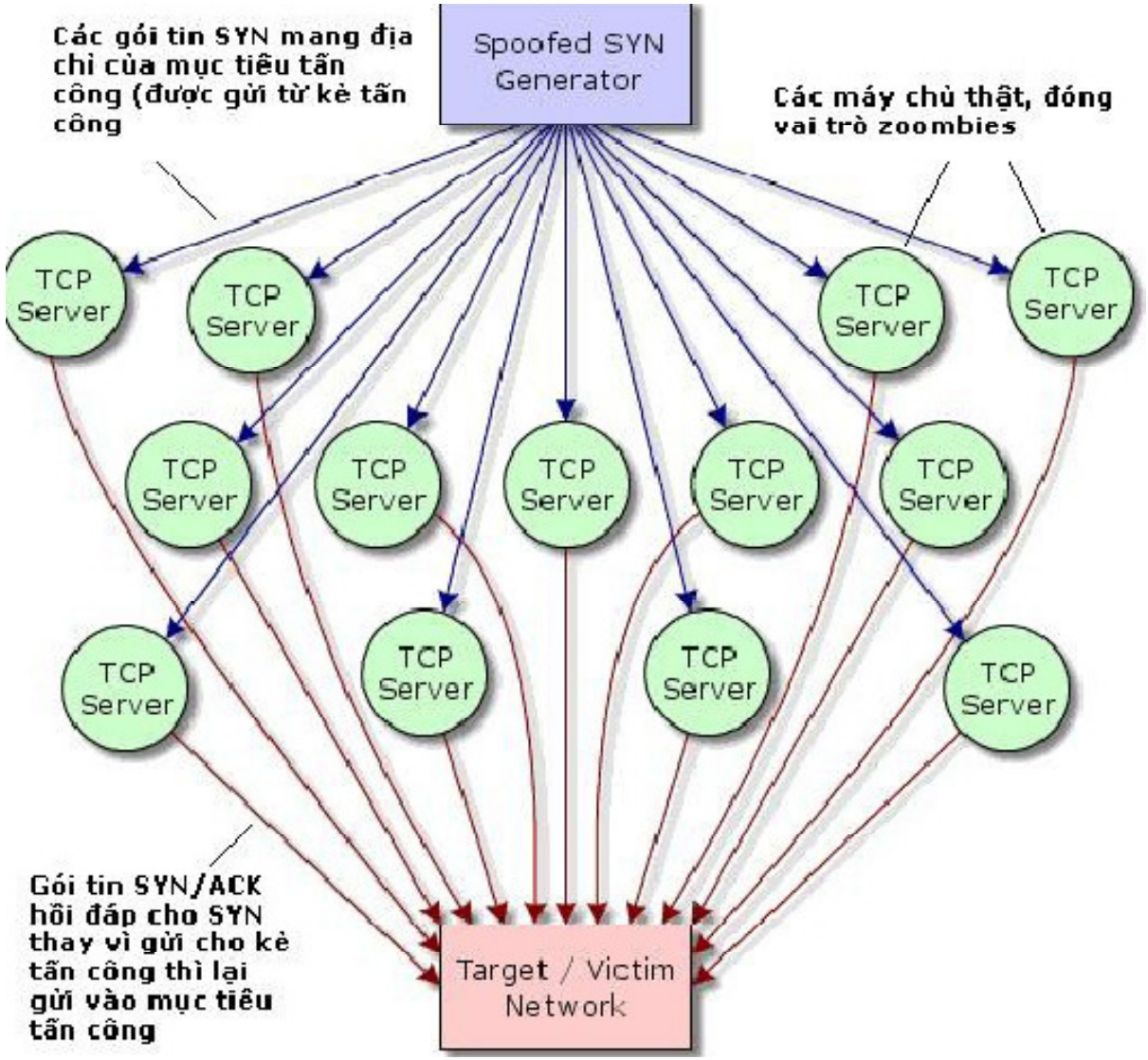
- Chiếm dụng và điều khiển nhiều máy tính/mạng máy tính trung gian (zombie)
- từ nhiều nơi
- để đồng loạt gửi ào ạt các gói tin (packet) với số lượng rất lớn
- nhằm chiếm dụng tài nguyên và làm tràn ngập đường truyền của một mục tiêu xác định nào đó.

Tấn công từ chối dịch vụ kiểu phân tán (DDoS)



Tấn công từ chối dịch vụ phản xạ nhiều vùng DRDoS

- Xuất hiện vào đầu năm 2002, là kiểu tấn công mới nhất, mạnh nhất trong họ DoS.
- Nếu được thực hiện bởi kẻ tấn công có tay nghề thì nó có thể hạ gục bất cứ hệ thống nào trên thế giới trong phút chốc.
- DRDoS là sự phối hợp giữa hai kiểu DoS và DDoS.
- Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy chủ, tức là làm tắc nghẽn hoàn toàn đường kết nối từ máy chủ vào xương sống của Internet và tiêu hao tài nguyên máy chủ.


Các gói tin SYN mang địa chỉ của mục tiêu tấn công (được gửi từ kẻ tấn công
Spoofed SYN Generator
Các máy chủ thật, đóng vai trò zoombies
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
TCP Server
Gói tin SYN/ACK hồi đáp cho SYN thay vì gửi cho kẻ tấn công thì lại gửi vào mục tiêu tấn công
Target / Victim Network

Tấn công từ chối dịch vụ phản xạ nhiều vùng DRDoS

- Với nhiều server lớn tham gia nên server mục tiêu nhanh chóng bị quá tải, bandwidth bị chiếm dụng bởi server lớn.
- Tính "nghệ thuật" là ở chỗ chỉ cần với một máy tính với modem 56kbps, một hacker lành nghề có thể đánh bại bất cứ máy chủ nào trong giây lát mà không cần chiếm đoạt bất cứ máy nào để làm phương tiện thực hiện tấn công.

Password attack

- Định nghĩa

  - Tấn công bằng mật khẩu là một kiểu phần mềm tấn công, trong đó kẻ tấn công cố gắng đoán mật khẩu hoặc crack mật khẩu mã hóa các file.

Password attack

- Tấn công reset mật khẩu
- Nghe lén mật khẩu
- Tấn công dò mật khẩu

Password attack

- Tấn công reset mật khẩu
  - Biết cơ chế mã hóa
  - Biết vị trí mã hóa
  - Khả năng truy xuất vào khu vực lưu trữ mã hóa
  - Tiến hành tính toán mật khẩu mới lưu vào vị trí lưu trữ

Password attack

- Nghe lén
  - Nghe lén, trộm mật khẩu lưu trữ vật lý
  - Nghe lén thông tin từ đó nhận được được mật khẩu không mã hóa
  - Nghe lén và lưu nhận mật khẩu đã mã hóa từ đó tiến hành gửi lại xác thực sau

Password attack

- Dò mật khẩu
  - Dò mật khẩu từ thông tin thu nhận được từ đối tượng bị tấn công
  - Dò tìm mật khẩu thông qua từ điển (đưa ra các mật khẩu có thể có theo thống kê)
  - Dò mật theo kiểu vét cạn, tất cả các trường hợp mật khẩu có thể có

Password attack

- Cách phòng tránh
  - Không cho phép user dùng cùng password trên các hệ thống.
  - Làm mất hiệu lực account sau một vài lần login không thành công.
  - Không dùng passwords dạng clear text
  - Dùng strong passwords

Misuse of Privilege Attack

- **Định nghĩa**
  - Misuse of Privilege Attack (Cuộc tấn công sử dụng sai các đặc quyền) là một loại phần mềm tấn công, trong đó kẻ tấn công sử dụng đặc quyền quản trị hệ thống để truy cập dữ liệu nhạy cảm. Loại tấn công này thường liên quan đến một nhân viên, với một số quyền quản trị trên một máy tính, một nhóm các máy móc hay một số phần của hệ thống mạng

Misuse of Privilege Attack

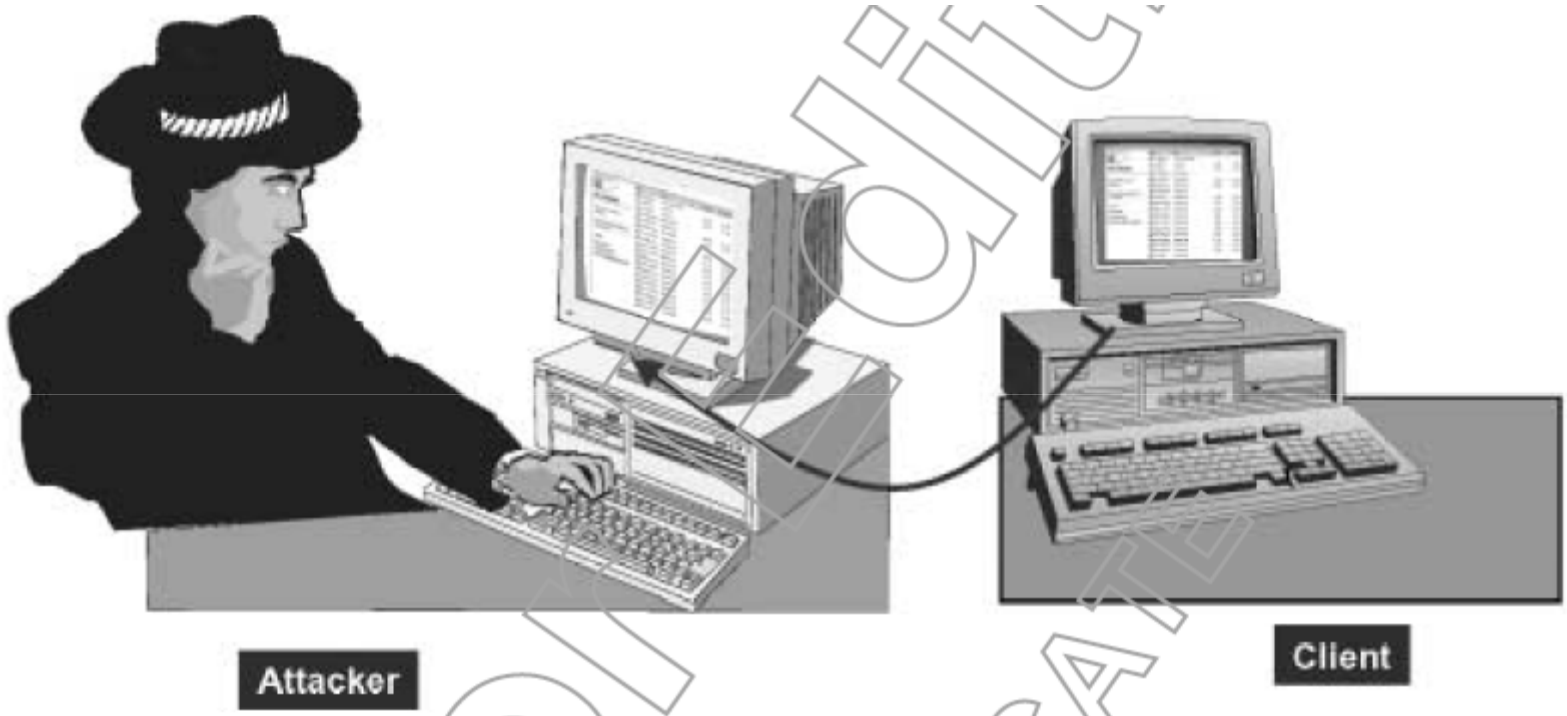


Figure 1-13: *Misuse of privilege attacks.*

Misuse of Privilege Attack

- Ví dụ

  Một quản trị mạng có khả năng truy cập vào các tập tin về thông tin cá nhân được lưu trữ trong cơ sở dữ liệu là một trong những tài nguyên quan trọng như là cơ sở dữ liệu nhận dạng của công an. Từ các tập tin về thông tin cá nhân này, anh ta có thể lấy tên đầy đủ, địa chỉ, số an sinh xã hội, và các dữ liệu khác, mà có thể có thể bán cho những người có thể sử dụng nó cho tội phạm liên quan đến gian lận nhận dạng.

Misuse of Privilege Attack

- Nguyên lý tấn công.

  Nhân viên có quyền truy cập hệ thống và các dữ liệu nhạy cảm, nhân viên này sử dụng các hình thức để ăn cắp dữ liệu nhạy cảm để bán ra ngoài:
- Lấy cắp dữ liệu nhạy cảm và chuyển ra ngoài hệ thống
- Cung cấp username, password cho những người ngoài hệ thống để xâm nhập hệ thống
- Cấp quyền truy cập cho những người ngoài hệ thống, dẫn đến mất mát dữ liệu

Misuse of Privilege Attack

- Cách phòng chống.
  - Mỗi nhân viên chỉ được cung cấp một quyền rất nhỏ để truy cập vào từng phần của hệ thống, không cho phép 1 nhân viên có quyền can thiệp vào hệ thống
  - Những chức năng quan trọng của hệ thống phải được đảm bảo do admin tin cậy của hệ thống quản lý

- Attacks Against the Default Security Configuration
- Tấn công vào cấu hình mặc định của hệ thống
  - Các mật khẩu mặc định
  - Cấu hình dịch vụ mặc định
  - Các thiết lập mặc định

- Software Exploitation Attacks
  - Tấn công vào lỗ hổng của các ứng dụng
  - Hệ điều hành
  - Các ứng dụng thông dụng của bên thứ 3 cung cấp: SQL server, Oracle server, IE, Firefox, …

AUDIT ATTACKS

- Tình huống cụ thể:
  - Một trong các bước quan trọng của hacker khi đã thâm nhập được vào Server là tìm cách xóa dấu tích của mình trong Audit Record.
- Có nhiều cách để xóa log này, 1 cách rất đơn giản và hiệu quả là dùng tool auditpol.
  - Auditpol không xóa file log mà nó chỉ disable chức năng audit.
  - Bạn cũng có thể enable chức năng này sau khi rút lui.

AUDIT ATTACKS

- Cách dùng auditpol rất dễ. Trước tiên bạn thử kiểm tra xem máy victim có bật chế độ audit không :

C:\auditpol IP_victim Running ... (X) Audit Enabled AuditCategorySystem = Success and Failure AuditCategoryLogon = Success and Failure AuditCategoryObjectAccess = Success and Failure AuditCategoryPrivilegeUse = Success and Failure AuditCategoryDetailedTracking = Success and Failure AuditCategoryPolicyChange = Success and Failure AuditCategoryAccountManagement = Success and Failure Unknown = Success and Failure Unknown = Success and Failure

AUDIT ATTACKS

- Nó sẽ hiện ra tất cả các chức năng của audit và tình trạng hiện thời của các chức năng đó (đang bật hay tắt) Cái mà bạn cần lưu tâm nhất là dòng thông báo đầu tiên " (X) Audit Enabled ".
- Như vậy audit trên máy victim đang hoạt động. Ta chỉ cần tắt audit bằng lệnh:

AUDIT ATTACKS

C:\auditpol IP_victim /disable Running ... Audit information changed successfully o-n IP_victim ... New audit policy o-n IP_victim ... (0) Audit Disabled AuditCategorySystem = No AuditCategoryLogon = No AuditCategoryObjectAccess = No AuditCategoryPrivilegeUse = No AuditCategoryDetailedTracking = No AuditCategoryPolicyChange = No AuditCategoryAccountManagement = No Unknown = No Unknown = No

Bây giờ thì bạn yên tâm tung hòanh trong máy victim mà không sợ bị theo dõi... Trước khi logoff trả lại trạng thái ban đầu cho audit .

Takeover Attacks

- Tấn công takeover là 1 kiểu tấn công phần mềm đó là nơi mà kẻ tấn công truy cập hệ thống , điều khiển máy chủ và kiểm soát hệ thống.
- Một kẻ tấn công có thể sử dụng bất kỳ các kiểu tấn công mà chúng ta xác định được cho đến nay để truy cập đươc hệ thống bao gốm IP spoofing và backdoor.

Malicious Software

Table 3-3 Malware differences

Type	Propagation	Examples
Virus	Copies itself into other executable programs and scripts	Melissa
Worm	Exploits vulnerabilities with the intent of propagating itself across the network	Code Red Code Red II Nimda
Trojan horse	Uses social engineering techniques to trick users into running the malware's executable	ILOVEYOU Naked Wife Anna Kournikova

Viruses

- Nó là các chương trình bản sao truyền đi bằng cách lây nhiễm tới các máy tính khác (Self-replicating programs that spread by “infecting” other programs)
- Gây tổn hại và tốn tiền của (Damaging and costly)

Table 3-4 Virus types

Type	Primary Period	Description
Boot sector	1980s to mid-90s	Spread by infecting floppy or hard disk boot sectors; when an infected disk is booted, the virus is loaded into memory and attempts to infect any and all floppy disks inserted into the computer
File infector	mid-90s	A class called "parasitic viruses" because they must infect other programs, file infectors copy themselves into other programs. When an infected file is executed, the virus is loaded into memory and tries to infect other executables. File types commonly infected include: *.exe, *.drv, *.dll, *.bin, *.ovl, *.sys, *.com
Multipartite	mid-90s	Propagated using both boot sector and file infector methods
Macro viruses	Current	Currently accounting for the vast majority of viruses, macro viruses are application specific as opposed to OS specific and propagate very rapidly via e-mail. Many macro viruses are Visual Basic scripts that exploit commonly used Microsoft applications such as Word, Excel, and Outlook.

Virus Databases

Table 3-5: Virus Databases

Network Associates (McAfee)	http://vil.nai.com/VIL/default.asp
Symantec	http://securityresponse.symantec.com/avcenter/vinfodb.html
Computer Associates	www3.ca.com/virus/encyclopedia.asp
Trend Micro	www.antivirus.com/vinfo/virusencyclo/

Evolution of Virus Propagation Techniques

Table 3-6 Evolution of virus propagation techniques

SKA	January 1999	Single mailer
Melissa	March 1999	Mass mailer targeting 50 recipients in a single activation
Babylonia	December 1999	Mass mailer using plug-in techniques
LoveLetter	May 2000	Mass mailer targeting all recipients in the victim's address book, in multiple activations
MTX	August 2000	Mass mailer incorporating file infector, sharing network, and backdoor features
Nimda	September 2001	Mass mailer, also incorporating file infector, sharing network, backdoor process, and IIS infector methods

Protecting Against Viruses

- Giải pháp để bảo vệ virus tấn công :
  - Cài chương trình diệt virus trên máy tính
  - Virus filters for e-mail servers
  - Tìm và diệt virus nhiễm trên các thiết bị mạng
- Instill good behaviors in users and system administrators
  - Keep security patches and virus signature databases up to date

Backdoor

- Remote access program surreptitiously installed on user computers that allows attacker to control behavior of victim's computer
- Also known as remote access Trojans
- Examples
  - Back Orifice 2000 (BO2K)
  - NetBus
- Detection and elimination
  - Up-to-date antivirus software
  - Intrusion detection systems (IDS)

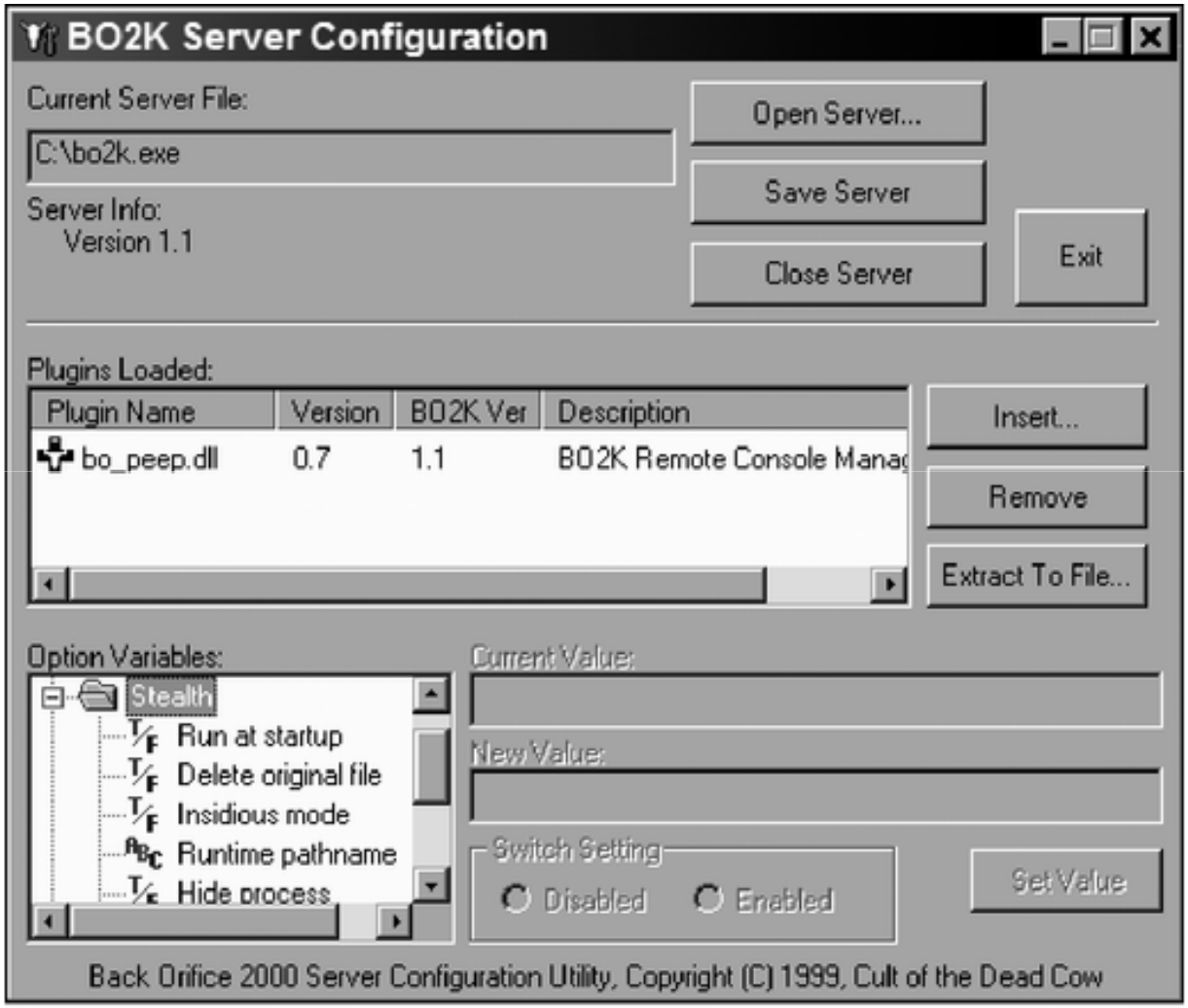


Figure 3-16 BO2K configuration screen

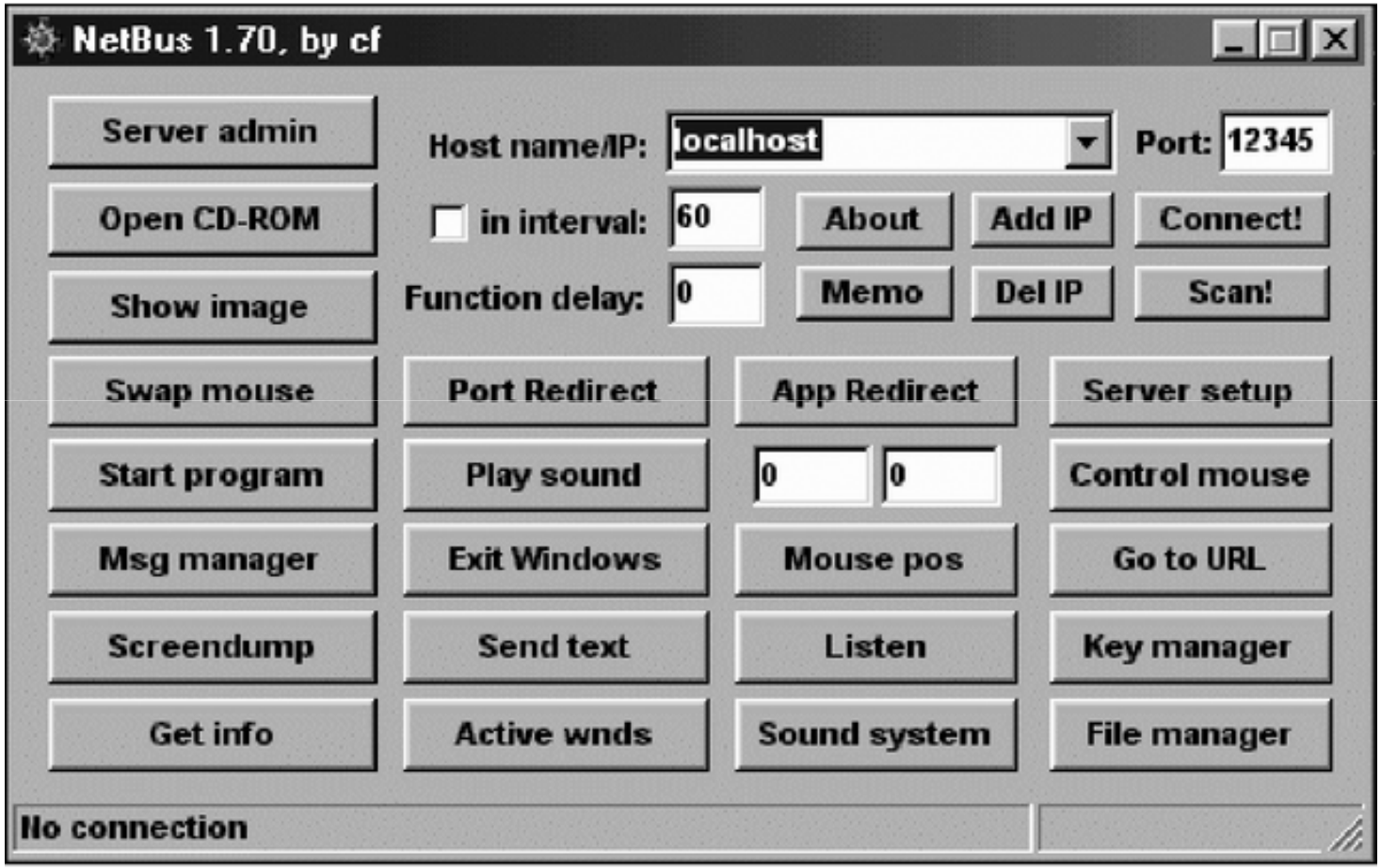


Figure 3-17 NetBus commands

Trojan Horses

- Class of malware that uses social engineering to spread
- Types of methods
  - Sending copies of itself to all recipients in user's address book
  - Deleting or modifying files
  - Installing backdoor/remote control programs

Logic Bombs

- Set of computer instructions that lie dormant until triggered by a specific event
- Once triggered, the logic bomb performs a malicious task
- Almost impossible to detect until after triggered
- Often the work of former employees
- For example: macro virus
  - Uses auto-execution feature of specific applications

Worms

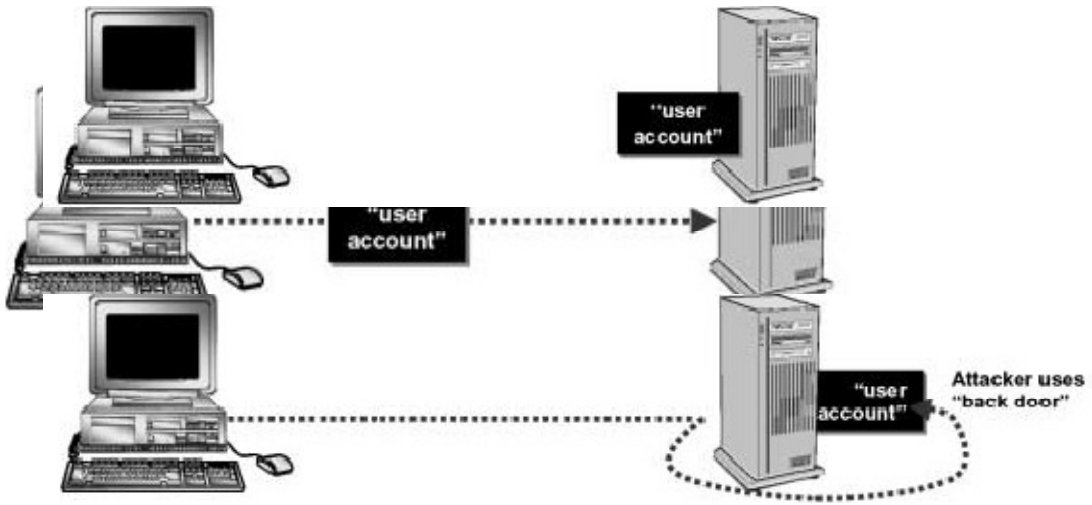
- Self-contained program that uses security flaws such as buffer overflows to remotely compromise a victim and replicate itself to that system
- Do not infect other executable programs
- Account for 80% of all malicious activity on Internet
- Examples: Code Red, Code Red II, Nimda

Defense Against Worms

- Latest security updates for all servers
- Network and host-based IDS
- Antivirus programs

Backdoor Attacks

- Tấn công backdoor là một kiểu tấn công phần mềm, đó là nơi mà kẻ tấn công tạo ra một cơ chế cho phép truy nhập vào một máy tính bằng cách sử dụng một phần mềm hoặc tạo thêm một tài khoản người dùng.


"user account"
"user account"
"user account"
Attacker uses "back door"

- nếu nó không được tìm thấy và gỡ bỏ, nó có thể tồn tại mãi mãi , lắng nghe trên một trong số các cổng (logic)

- Tạo ra cho kẻ tấn công một con đường dễ dàng vào hệ thống và có thể thực hiện bất cứ một lệnh nào

- Thông thường thì backdoor dược thực hiện qua việc sử dụng một số Trojan horse hoặc một số mã độc hại khác, tấn công backdoor thường không thể phát hiện bởi chúng không để lại bất cứ dấu vết gì.

Mục đích

- Lấy thông tin của các tài khoản cá nhân như: Email, Password, Usernames, dữ liệu mật …
- Lây nhiễm các phần mềm ác tính khác như là virus
- Đọc lén các thông tin cần thiết và gửi báo cáo đến nơi khác (xem thêm phần mềm gián điệp)
- Cài đặt lén các phần mềm chưa được cho phép

Cách phòng chống

- Cách hữu hiệu nhất là đừng bao giờ mở các đính kèm được gửi đến một cách bất ngờ. Khi các đính kèm không được mở ra thì Trojan horse cũng không thể hoạt động. Cẩn thận với ngay cả các thư điện tử gửi từ các địa chỉ quen biết. Trong trường hợp biết chắc là có đính kèm từ nơi gửi quen biết thì vẫn cần phải thử lại bằng các chương trình chống virus trước khi mở nó.

Tấn công mạng máy tính

- Port scan attack
- Eavesdropping attack
- IP spoofing attack
- Man-in-the-middle Attack
- Replay attack
- Hijacking Attack
- Denial of Service / Distributed Denial of Service (DoS/DDoS) Attacks
- Các loại tấn công phần mềm