PHÁT HIỆN TẤN CÔNG MẠNG

Đỗ Thanh Nghị
dtnghi@cit.ctu.edu.vn

01-2018

Nội dung

- Giới thiệu
- Hệ thống phát hiện xâm nhập mạng
- Phát hiện xâm nhập mạng với Snort
- Xây dựng luật cho Snort

Tài liệu tham khảo

- B. Caswell, J. Beale, A. Baker, "*Snort IDS and IPS Toolkit*", Syngress, 2007
- J. Babbin, S. Biles, A.D. Orebaugh, "*Snort Cookbook*", O'Reilly, 2005
- M. Gregg, "*The Network Security Test Lab: A Step-by-Step Guide*", Wiley, 2015
- TutorialPoints, "*Network Security Tutorial*", 2017
- R. Bejtlich, "*The Practice of Network Security Monitoring: Understanding Incident Detection and Response*", No Starch Press, 2013

Tài liệu tham khảo

- W. Stallings and L. Brown, "*Computer Security: Principles and Practice*", Pearson; 3 edition, 2014
- C. Scott, P. Wolfe, B. Hayes, "*Snort For Dummies*", Wiley, 2004
- R.U. Rehman, "*Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID*", Prentice Hall, 2003
- Cisco, "*SNORT® User Manual*", 2017
- Cisco, "Snort - Network Intrusion Detection & Prevention System", 2017. https://www.snort.org

Tổ chức lớp học

- Lý thuyết: 30t (sinh viên không sử dụng điện thoại trong giờ học)
- Thực hành: 30t (tính điểm từng buổi)
- Báo cáo chuyên đề: 20%
- Điểm thực hành: 30%
- Thi cuối kỳ: 50%, tự luận

Nội dung

- **Giới thiệu**
- Hệ thống phát hiện xâm nhập mạng
- Phát hiện xâm nhập mạng với Snort
- Xây dựng luật cho Snort

Giới thiệu

- Mạng máy tính được sử dụng phổ biến
- Hiệu quả để chia sẻ, trao đổi thông tin
- Một nhân viên sở hữu 1 máy tính
- Mạng máy tính của tổ chức, tập đoàn, công ty có số lượng máy tính tương ứng số nhân viên của công ty
- Các máy tính trong mạng
  - Phân tán, quản lý phi tập trung, sử dụng nhiều hệ điều hành, phần mềm, phần cứng, nghi thức khác nhau
  - Kiến thức người dùng khác nhau
  - Cùng nối kết đến mạng Internet
- Dễ trở thành mục tiêu của các cuộc tấn công mạng

Giới thiệu

- Theo Reuters, báo cáo từ hai công ty bảo hiểm lớn của Anh Lloyd's và Cyence hôm 17/7/2017
  - Ước tính mức thiệt hại kinh tế từ một cuộc tấn công mạng lớn trên thế giới có thể dao động từ 4.6 lên đến 53 tỉ USD
  - Chi phí kinh tế toàn cầu bị tổn thất từ vụ tấn công bằng mã độc tống tiền "WannaCry" hồi tháng 5/2017, tại hơn 100 quốc gia, vùng lãnh thổ đã lên tới 8 tỉ USD
  - Sự tấn công của virus "NotPetya" được lan truyền từ Ukraine ra toàn cầu ngay sau "WannaCry", tận dụng lỗ hổng EternalBlue của Windows, chiếm quyền kiểm soát, mã hóa dữ liệu và đòi tiền chuộc để giải mã, với chi phí thiệt hại lên đến 850 triệu USD
  - Phần lớn thiệt hại là do các hoạt động kinh doanh bị gián đoạn và chi phí sửa chữa các hệ thống máy tính bị nhiễm virus

Giới thiệu

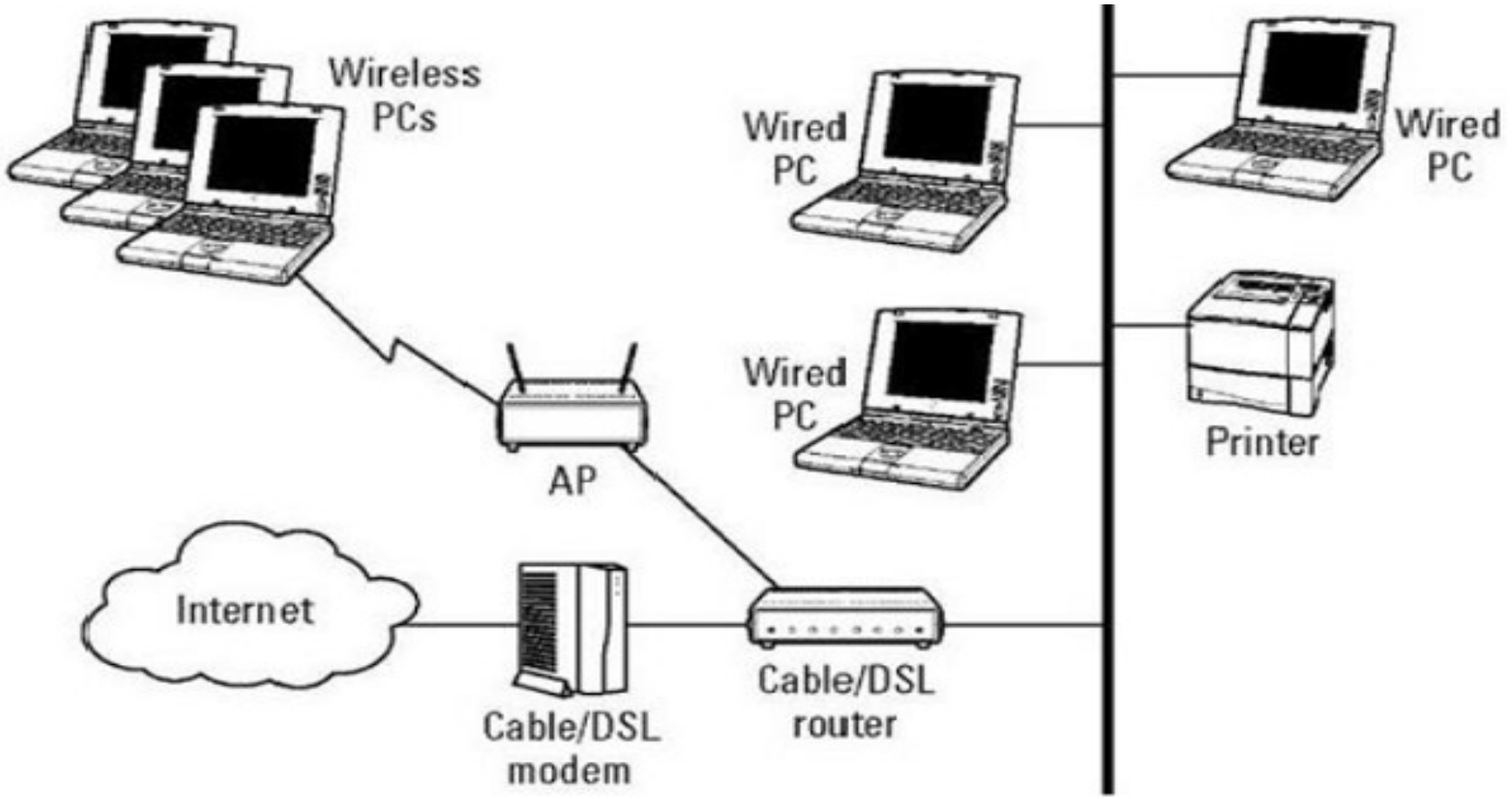
- Các cuộc tấn công DDoS nổi tiếng trong lịch sử
  - Năm 2000, website nổi tiếng như Yahoo, eBay, eTrade, Amazon và CNN trở thành nạn nhân của DDoS
  - Tháng 02/2001, máy chủ của Cục tài chính Ireland bị một số sinh viên Đại học Maynooth ở nước này tấn công DDoS
  - Ngày 15/08/2003, Microsoft chịu đợt tấn công DoS làm gián đoạn websites trong vòng 2 giờ
  - Tháng 02/2007, hơn 10000 máy chủ của game trực tuyến Return to Castle Wolfenstein, Halo, Counter-Strike, … bị nhóm RUS tấn công với hệ thống điều khiển đặt tại Nga, Uzbekistan và Belarus

Giới thiệu

- Các cuộc tấn công DDoS nổi tiếng trong lịch sử
  - Tháng 08/2009, các vụ DDoS nhắm tới các trang mạng xã hội như Facebook, Twitter, LiveJournal và một số website của Google được thực hiện để "khóa miệng" blogger tên Cyxymu ở Georgia
  - Ngày 28/11/2010, WikiLeaks bị tê liệt vì DDoS ngay khi họ chuẩn bị tung ra những tài liệu mật của chính phủ Mỹ
  - Ngày 07/12/2010, nhóm hacker có tên Anonymous đánh sập website Visa.com, Mastercard và PayPal để trả đũa cho việc chủ WikiLeaks bị tạm giam ở Anh
  - Ngày 03/3/2011, dịch vụ blog nổi tiếng WordPress bị tấn công
  - Ngày 04/3/2011, 40 trang web của các cơ quan chính phủ Hàn Quốc bị tê liệt vì DDoS

Giới thiệu

Giới thiệu


Wireless
PCs
AP
Internet
Cable/DSL
modem
Cable/DSL
router
Wired
PC
Wired
PC
Wired
PC
Printer

Giới thiệu

- Lỗ hổng của mạng có dây hay không dây là truy cập không chứng thực đến mạng
- Kẻ tấn công thực hiện kết nối từ thiết bị của anh ta đến mạng thông qua cổng hub/switch không an toàn
- Mạng kết nối không dây là ít an toàn hơn mạng có dây do tính dễ truy xuất không dây
- Sau khi truy cập đến mạng, kẻ tấn công sẽ khai thác lỗ hổng để thực hiện các nhiệm vụ tấn công

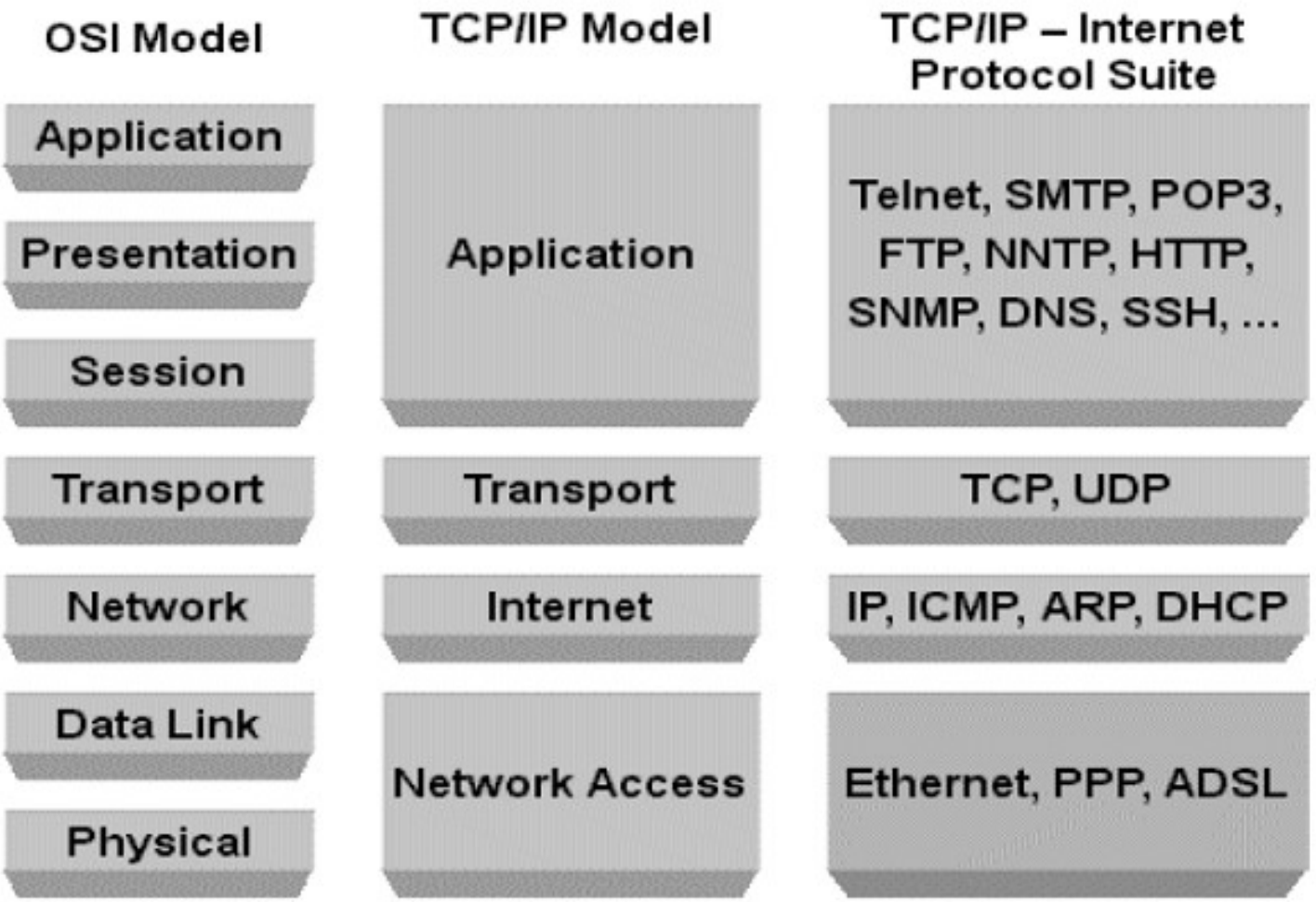
Giới thiệu

- Tấn công mạng:
  - Thu thập các gói tin để ăn cắp các thông tin có giá trị
  - Từ chối dịch vụ cho người dùng hợp pháp trên mạng bằng cách làm tràn các phương tiện truyền thông mạng với các gói giả mạo
  - Giả mạo địa chỉ vật lý (MAC) của các máy chủ hợp pháp và sau đó ăn cắp dữ liệu hoặc tiếp tục tung ra một cuộc tấn công dạng "người-trung-gian" (man-in-the-middle)

Giới thiệu

- Nghi thức mạng
  - Tập hợp các quy tắc điều khiển truyền thông giữa các thiết bị được kết nối trên mạng
  - Chúng bao gồm các cơ chế tạo kết nối, các quy tắc định dạng để đóng gói dữ liệu cho các gói tin được gửi và nhận
  - Một số nghi thức mạng máy tính đã được phát triển cho từng mục đích cụ thể
  - Nghi thức TCP/IP: phổ biến và được sử dụng rộng rãi

Giới thiệu


OSI Model
TCP/IP Model
TCP/IP – Internet Protocol Suite
Application
Presentation
Session
Application
Telnet, SMTP, POP3, FTP, NNTP, HTTP, SNMP, DNS, SSH, ...
Transport
Transport
TCP, UDP
Network
Internet
IP, ICMP, ARP, DHCP
Data Link
Physical
Network Access
Ethernet, PPP, ADSL

Giới thiệu

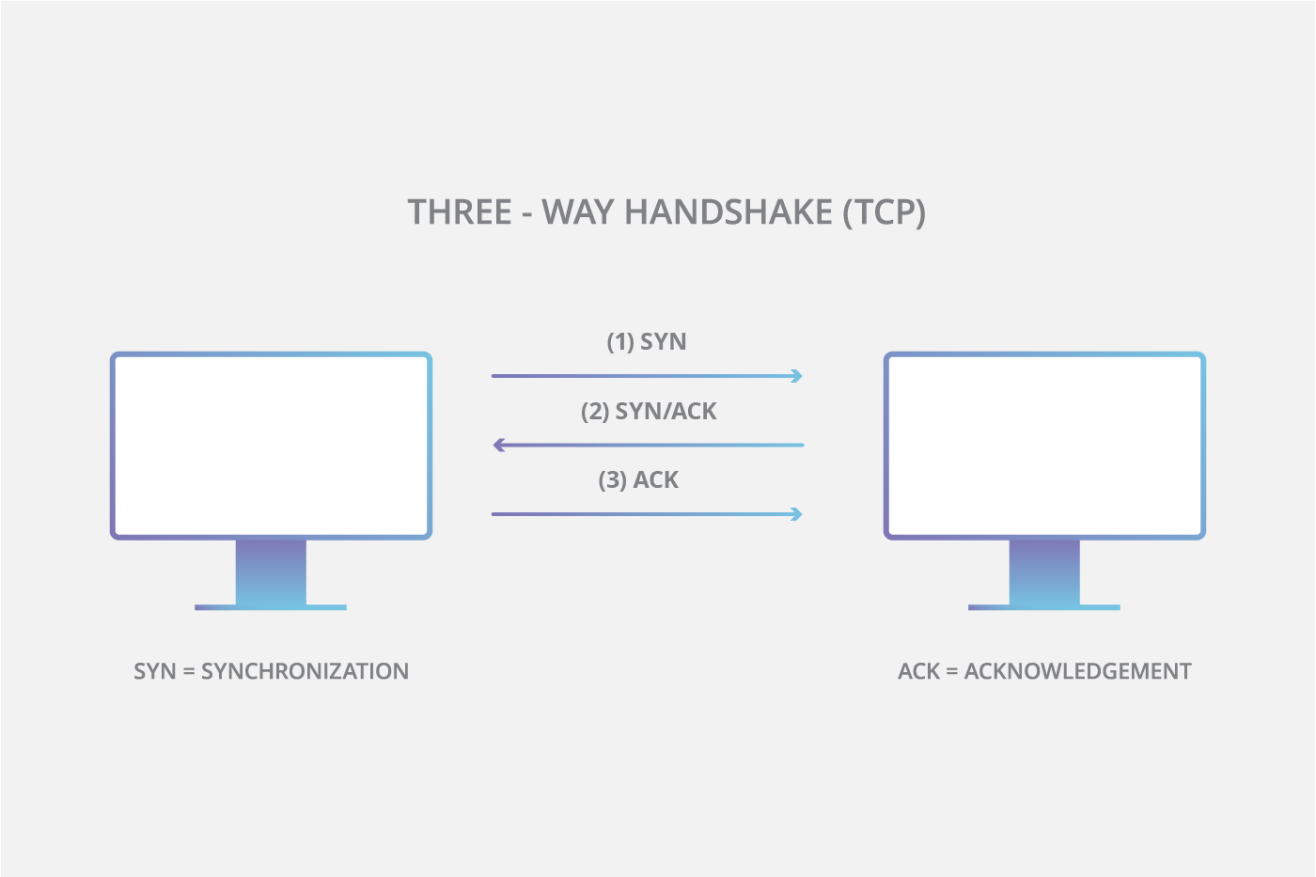
- Nghi thức TCP/IP
  - Ra đời vào 1980, được sử dụng phổ biến trong kết nối mạng
  - Nhưng ít được quan tâm đến vấn đề an ninh
  - Được phát triển cho một giao tiếp trong mạng tin cậy giới hạn
  - Trở thành nghi thức truyền thông Internet không an toàn trong thời gian qua

Giới thiệu

- Một vài ví dụ về lỗ hổng của TCP/IP
  - HTTP là một nghi thức tầng ứng dụng của TCP/IP được dùng để truyền các tập tin (các trang web) từ máy chủ web. Do dữ liệu được truyền tải dạng văn bản thuần túy nên kẻ đột nhập có thể dễ dàng đọc các gói dữ liệu trao đổi giữa máy chủ và máy khách
  - Một lỗ hổng HTTP khác là sự xác thực yếu giữa máy khách và máy chủ web trong quá trình khởi tạo một phiên (session). Lỗ hổng này có thể dẫn đến cuộc tấn công chiếm quyền truy cập phiên, kẻ tấn công đánh cắp một phiên HTTP của người dùng hợp pháp

Giới thiệu

- Nghi thức bắt tay TCP/IP

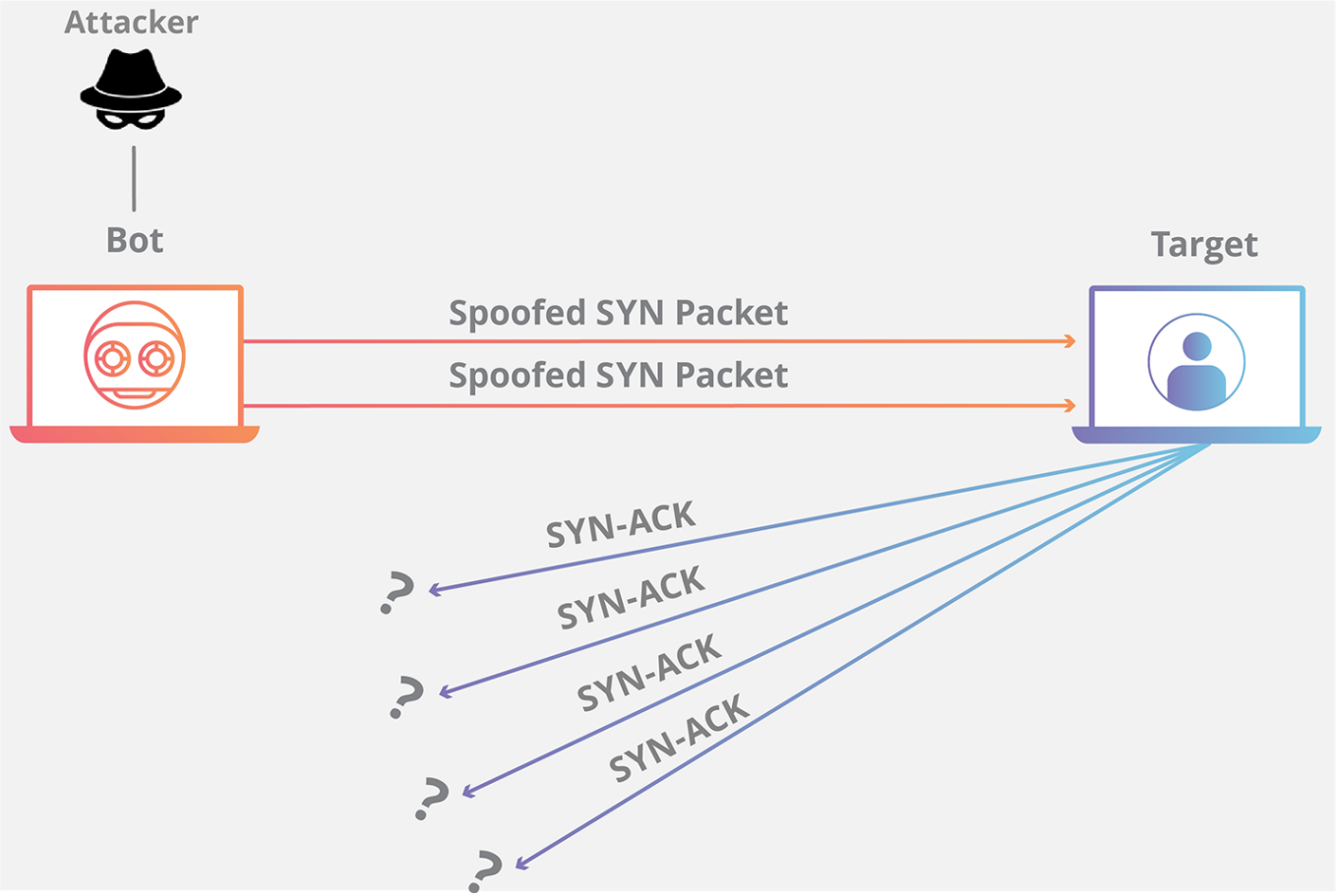


Giới thiệu

- Một vài ví dụ về lỗ hổng của TCP/IP
  - Lỗ hổng của nghi thức TCP là bắt tay three-way để thiết lập kết nối. Kẻ tấn công có thể mở cuộc tấn công từ chối dịch vụ "SYN-flooding" để khai thác lỗ hổng này. Anh ta thiết lập rất nhiều phiên mở dang dở bằng cách không bắt tay. Điều này dẫn đến quá tải máy chủ và cuối cùng máy chủ gục ngã
  - Tầng IP dễ bị ảnh hưởng bởi nhiều lỗ hổng. Thông qua sửa đổi header của nghi thức IP, kẻ tấn công có thể khởi chạy cuộc tấn công giả mạo IP.

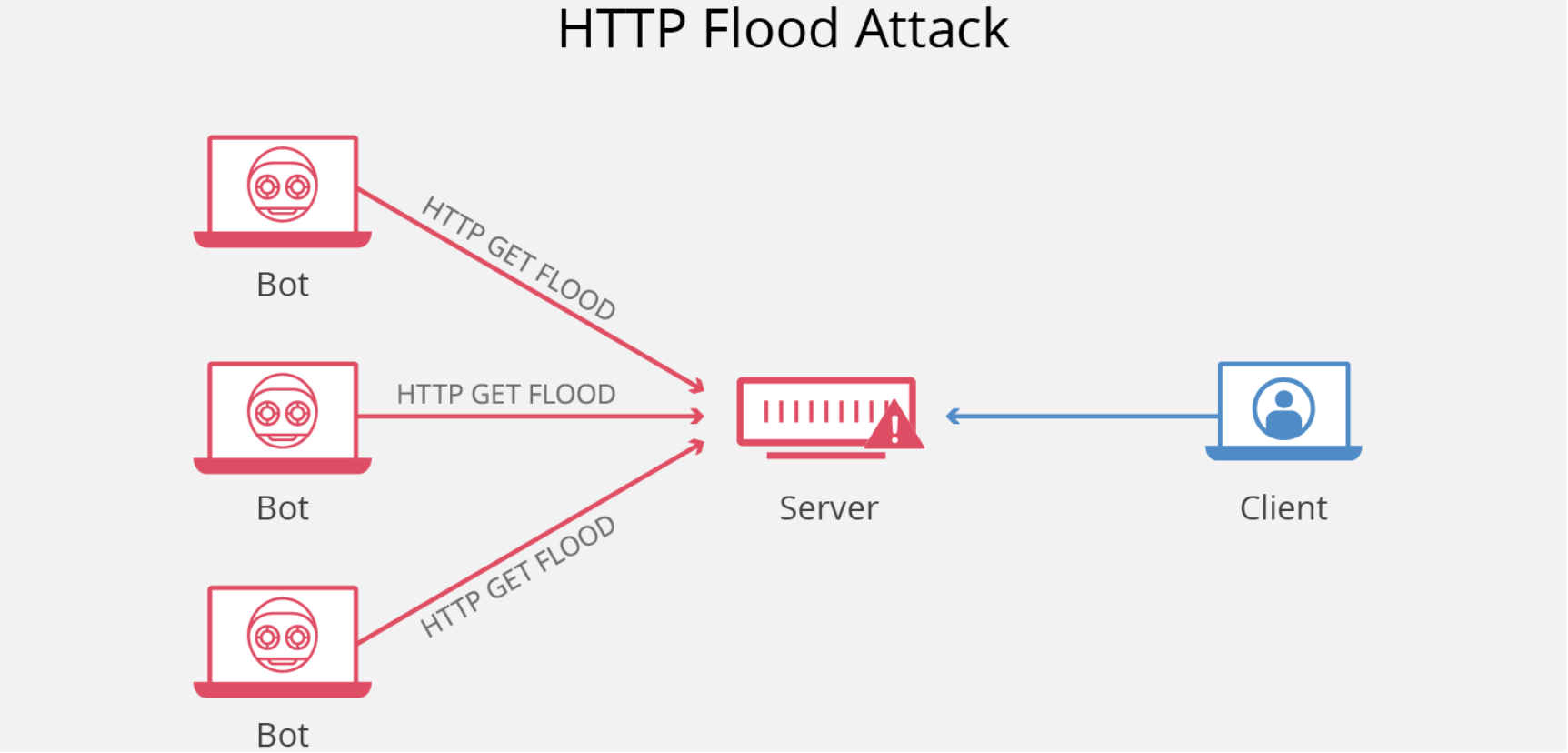
Giới thiệu

- SYN Flood



Giới thiệu

- HTTP Flood

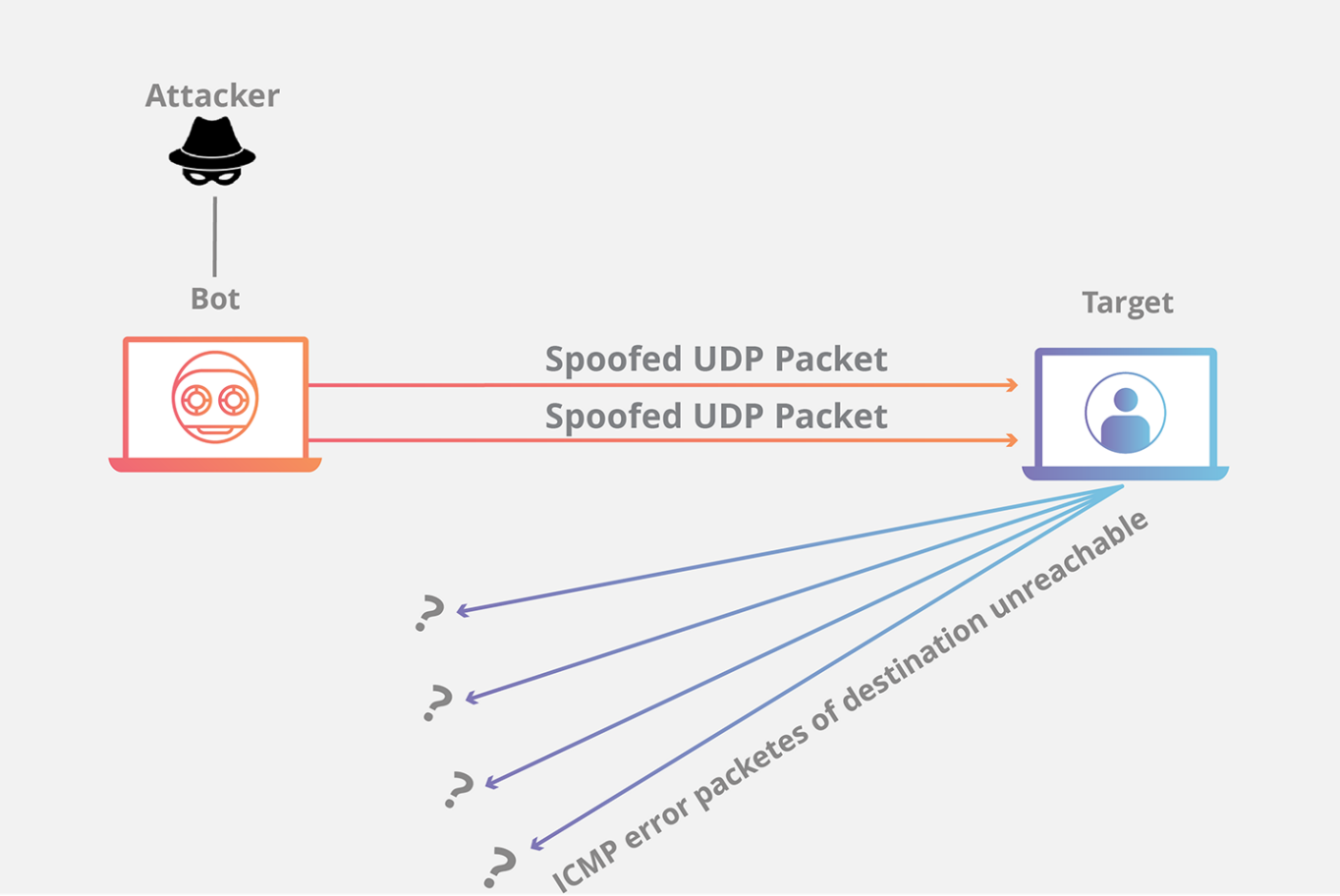


Giới thiệu

- Nghi thức UDP
  - Nghi thức kết nối không tin cậy
  - Một cuộc tấn công có thể được bắt đầu bằng cách gửi một số lượng lớn các gói tin UDP tới cổng ngẫu nhiên trên một máy chủ từ xa và kết quả là các máy chủ ở xa sẽ:
    - Kiểm tra các ứng dụng với cổng;
    - Thấy rằng không có ứng dụng nghe ở cổng;
    - Trả lời với một ICMP Destination Unreachable gói

Giới thiệu

- UDP Flood

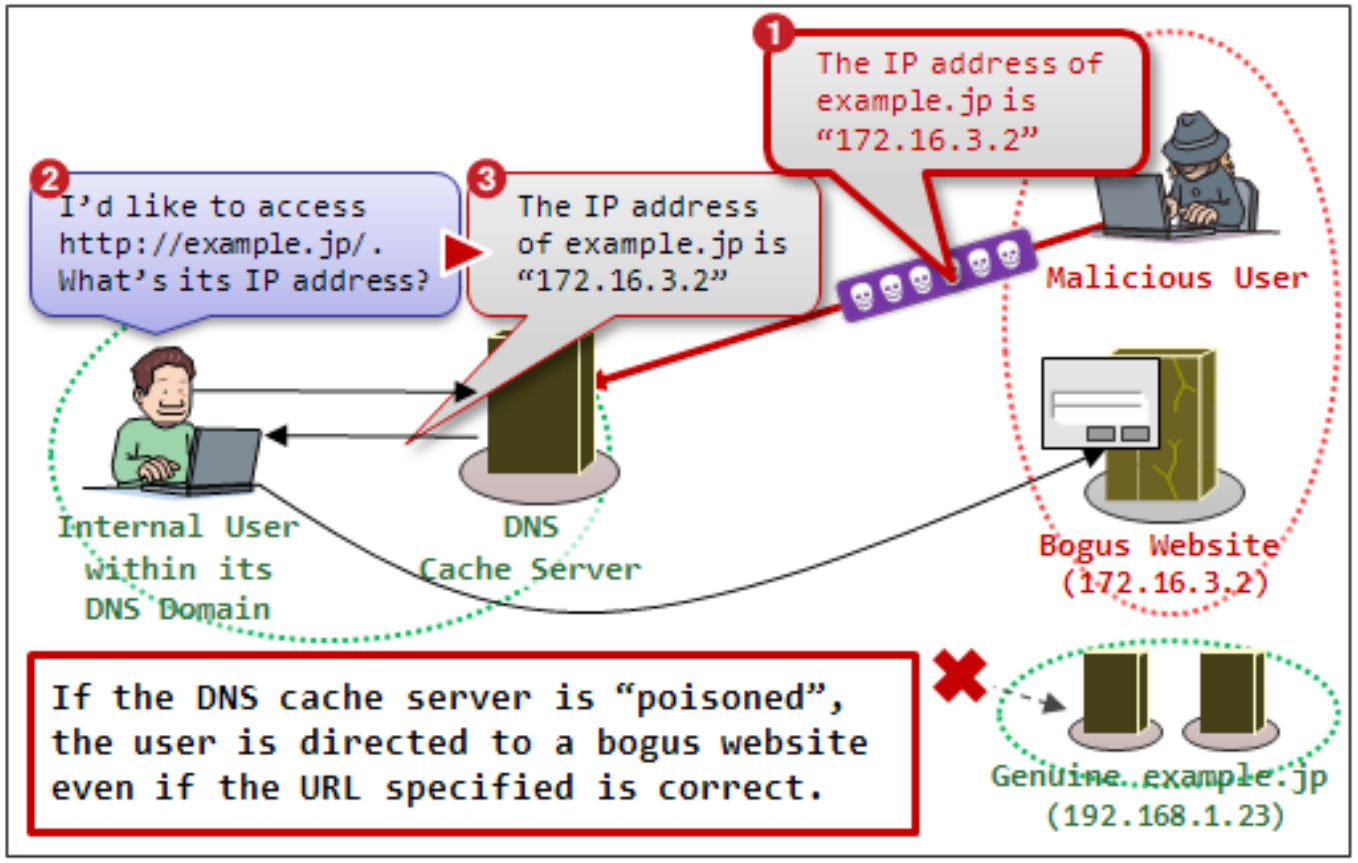


Giới thiệu

- Nghi thức DNS
  - Được sử dụng để giải tên miền ra địa chỉ IP. Người dùng mạng phụ thuộc vào chức năng DNS trong quá trình duyệt Internet bằng cách gõ một URL trong trình duyệt web
  - Trong cuộc tấn công vào DNS, mục tiêu của kẻ tấn công là chỉnh sửa một bản ghi DNS hợp lệ để nó giải tên miền hợp lệ thành một địa chỉ IP sai. Điều này có thể hướng tất cả lưu lượng truy cập cho đến máy tính sai địa chỉ IP. Kẻ tấn công có thể khai thác lỗ hổng nghi thức DNS hoặc thỏa hiệp với máy chủ DNS để thực hiện một cuộc tấn công

Giới thiệu

- DNS giả mạo



Giới thiệu

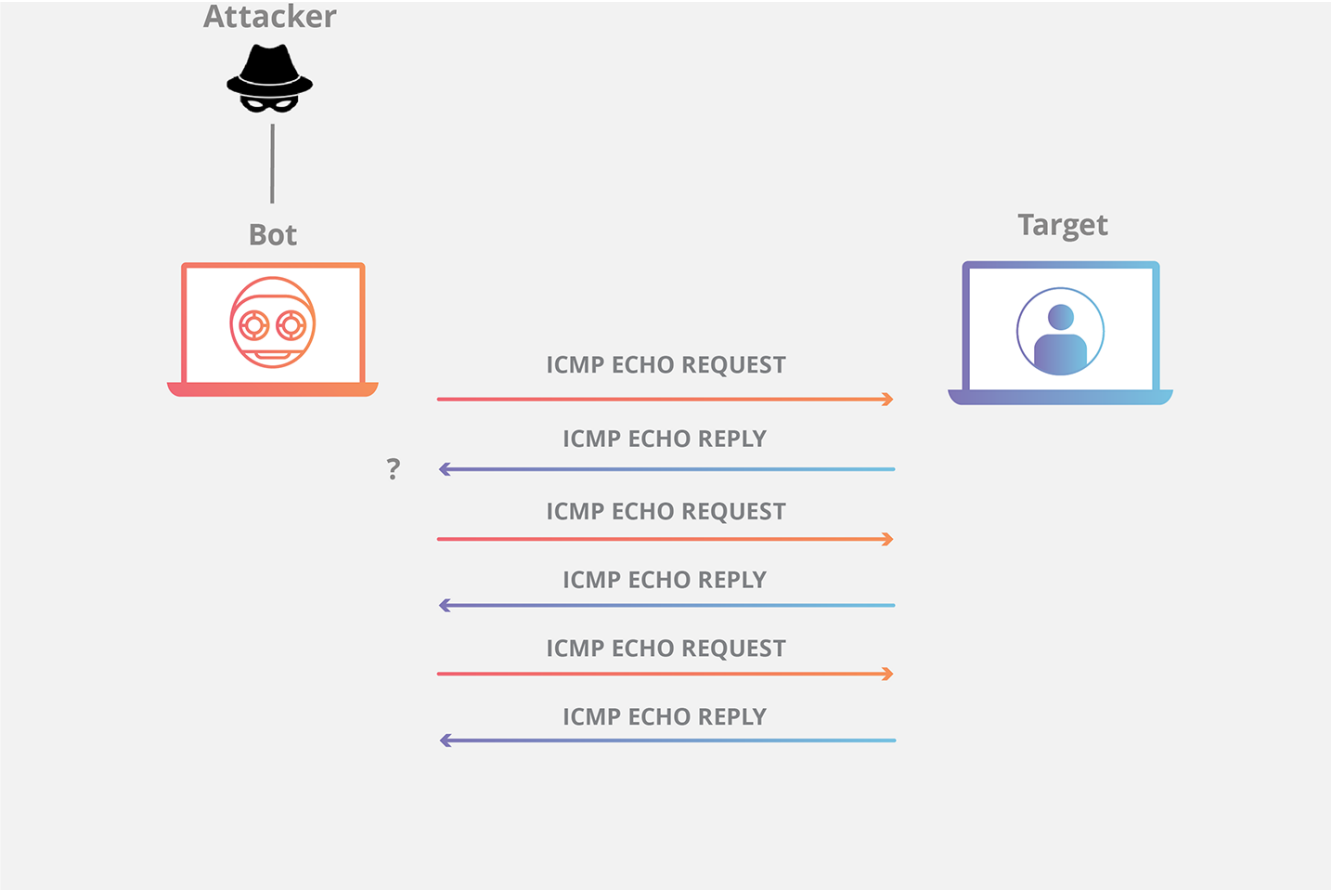
- Nghi thức ICMP
  - Nghi thức quản lý mạng cơ bản của mạng TCP/IP. ICMP được sử dụng để gửi thông báo lỗi và kiểm soát trạng thái của các thiết bị nối mạng
  - ICMP là một phần tích hợp trong cài đặt mạng IP và do đó ICMP hiện diện trong quá trình thiết lập mạng.
  - ICMP có các lỗ hổng riêng và có thể bị khai thác để khởi động cuộc tấn công trên mạng

Giới thiệu

- Lỗ hổng ICMP
  - ICMP cho phép kẻ tấn công thực hiện cuộc thám sát mạng để xác định topo mạng và đường dẫn vào mạng. ICMP thăm dò và khám phá tất cả các địa chỉ IP của máy chủ đang tồn tại trong mạng
  - Trace route là một tiện ích phổ biến của ICMP được sử dụng để lập bản đồ mạng bằng cách mô tả đường dẫn theo thời gian thực từ máy khách đến máy chủ từ xa
  - Kẻ tấn công có thể tấn công từ chối dịch vụ bằng cách gửi các gói tin ping IPMP vượt quá 65.535 bytes đến máy chủ => cắt nhỏ => khiến máy chủ xử lý nhiều và máy chủ sụp đổ
- Còn rất nhiều lỗ hổng của các nghi thức ARP, DHCP, SMTP, HTTP, etc.

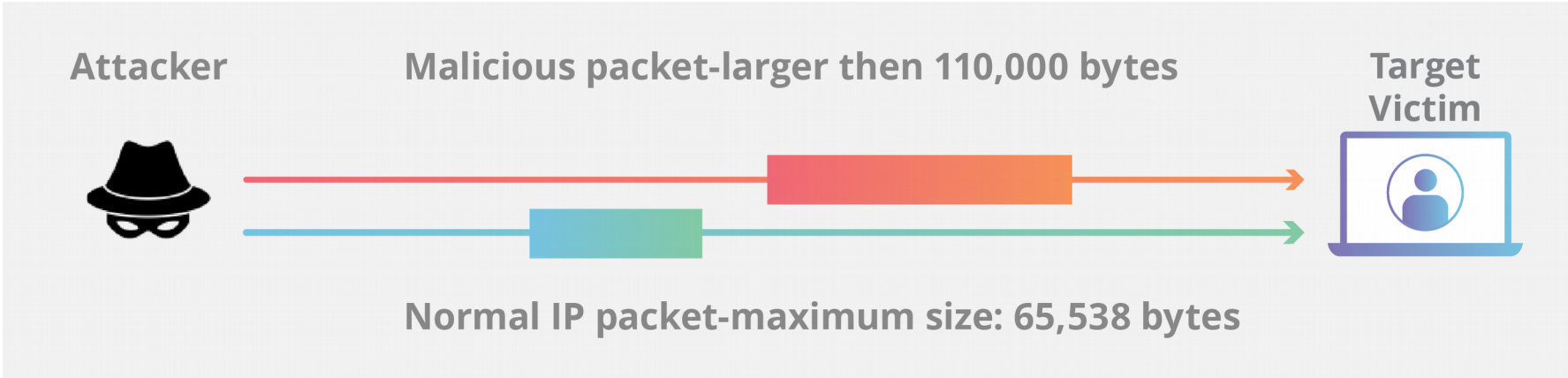
Giới thiệu

- Ping (ICMP) Flood



Giới thiệu

- Ping of Death

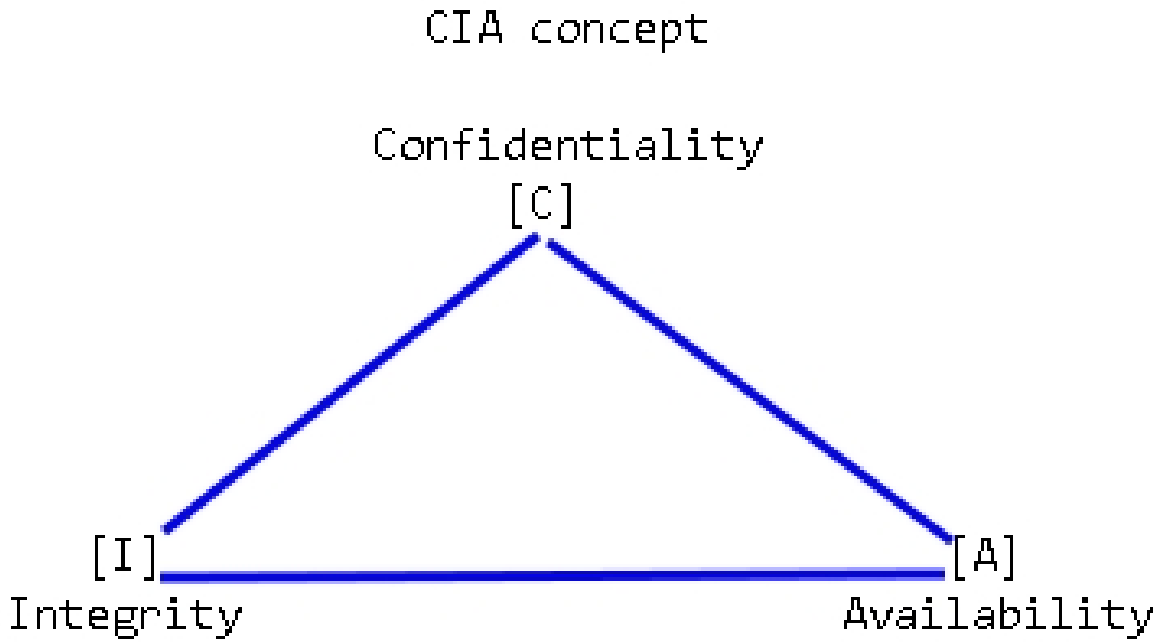


Giới thiệu

- Mục tiêu an ninh mạng
  - Tồn tại nhiều lỗ hổng trong mạng. Do đó, trong quá trình truyền, dữ liệu rất dễ bị tấn công. Kẻ tấn công có thể nhắm mục tiêu kênh truyền thông, thu thập dữ liệu và đọc cùng hoặc đưa lại một thông điệp giả để đạt được mục tiêu bất chính của anh ta
  - An ninh mạng không chỉ quan tâm đến sự an toàn của máy tính ở mỗi đầu của chuỗi truyền thông; mà còn nhằm mục đích đảm bảo rằng toàn bộ mạng là an toàn
  - An ninh mạng đòi hỏi phải bảo vệ khả năng sử dụng, độ tin cậy, tính toàn vẹn, và sự an toàn của mạng và dữ liệu.
  - An ninh mạng hiệu quả phải đánh bại nhiều mối đe dọa khác nhau khi mạng bị xâm nhập

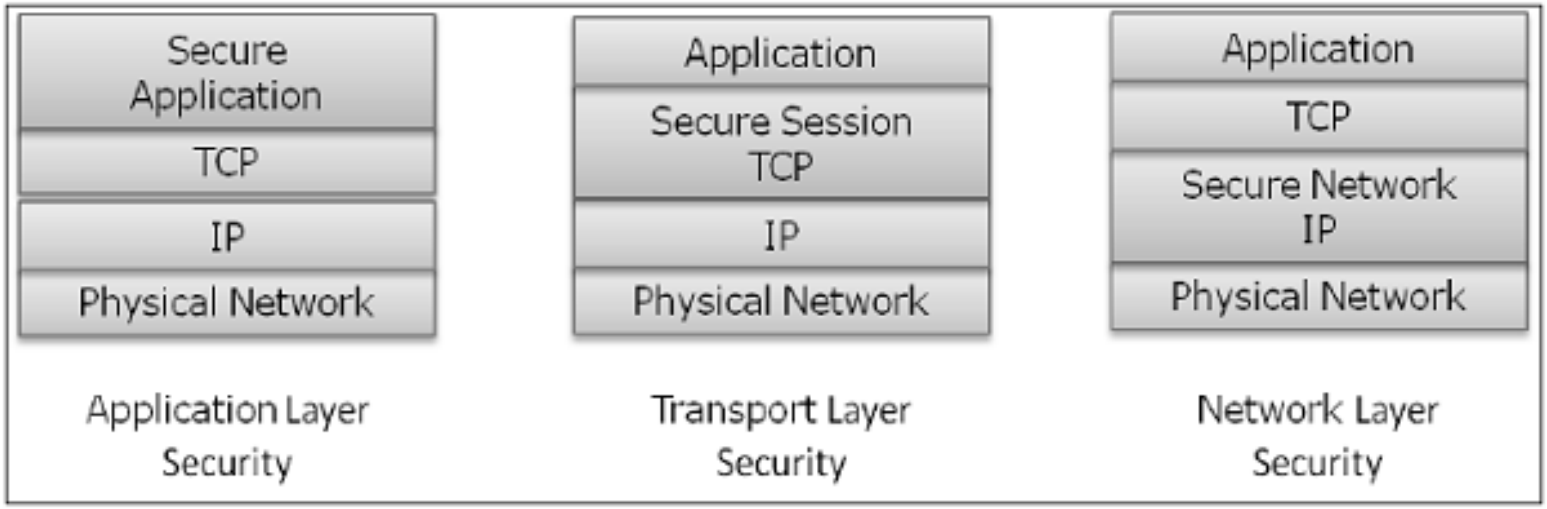
Giới thiệu

- Mục tiêu an ninh mạng
  - Phải đảm bảo được ba tiêu chí quan trọng: bảo mật, tính toàn vẹn và tính khả dụng. Ba trụ cột của An ninh Mạng thường được biểu diễn dưới dạng tam giác CIA



Giới thiệu

- Mục tiêu an ninh mạng
  - Bảo vệ dữ liệu chống lại các tấn công khi truyền tải trên mạng
  - Nhiều nghi thức bảo mật được thiết kế, cung cấp ít nhất các mục tiêu chính: các bên có thể đàm phán tương tác để xác thực lẫn nhau, thiết lập khoá bí mật trước khi trao đổi thông tin trên mạng, trao đổi thông tin dưới dạng mã hoá



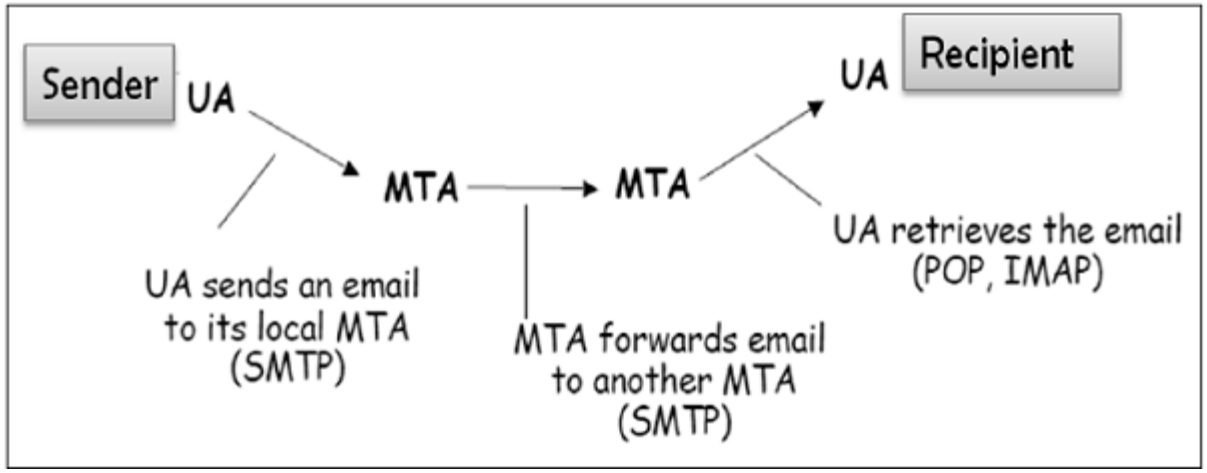
Giới thiệu

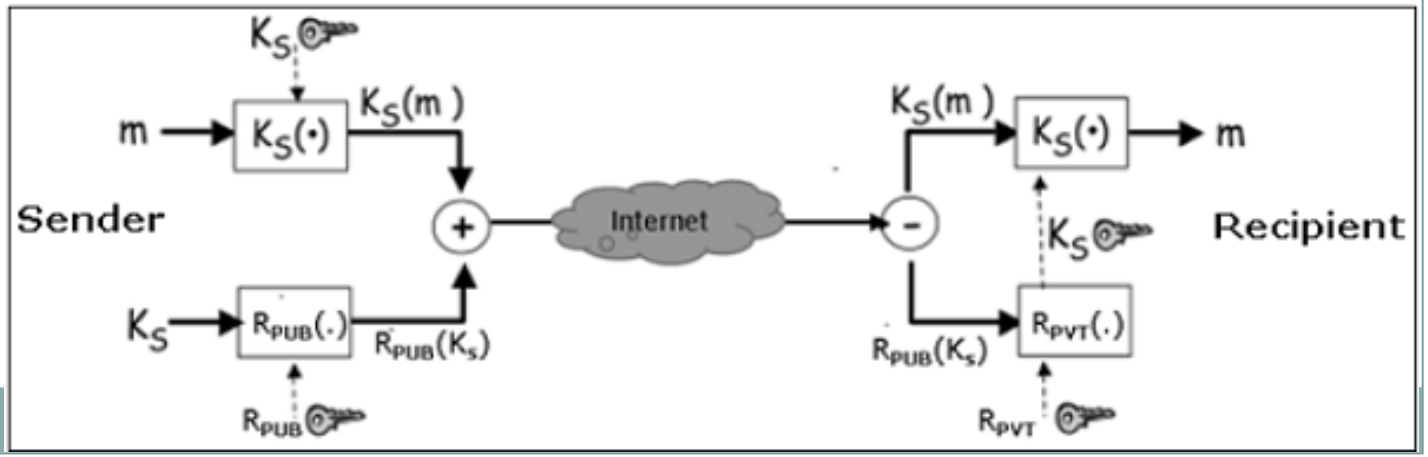
- Nghi thức an ninh

Layer	Communication Protocols	Security Protocols
Application Layer	HTTP FTP SMTP	PGP. S/MIME, HTTPS
Transport Layer	TCP /UDP	SSL, TLS, SSH
Network Layer	IP	IPsec

Giới thiệu

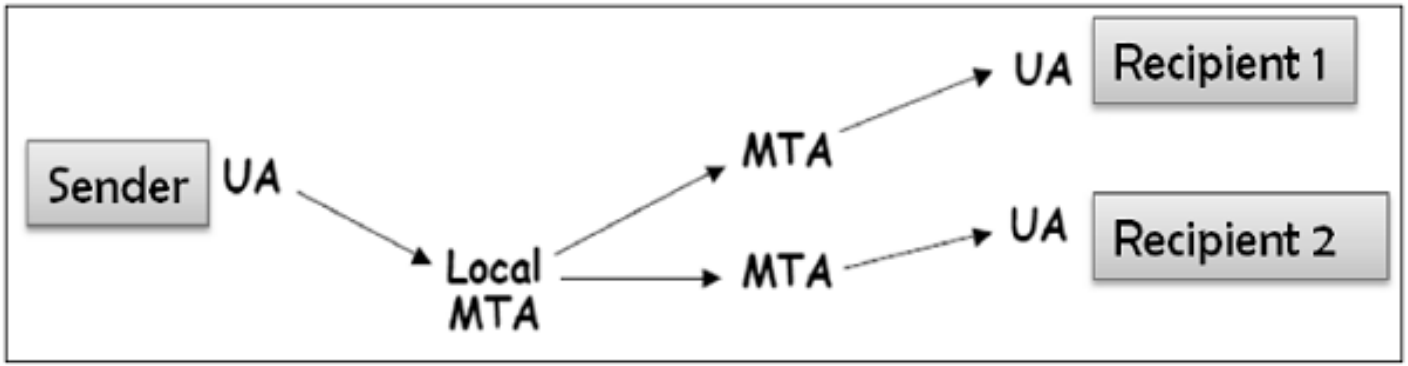
- Dịch vụ E-Mail Security (1-tới-1)

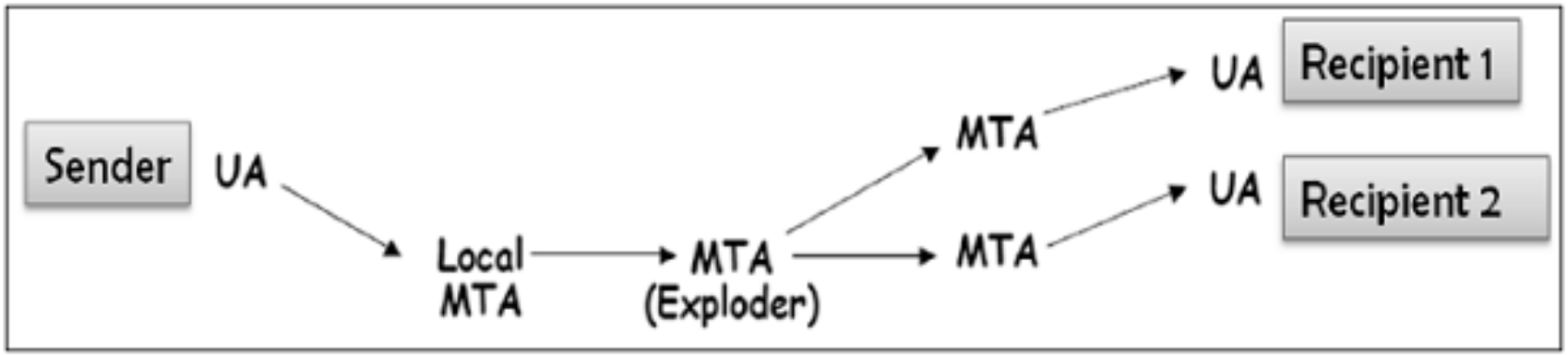




Giới thiệu

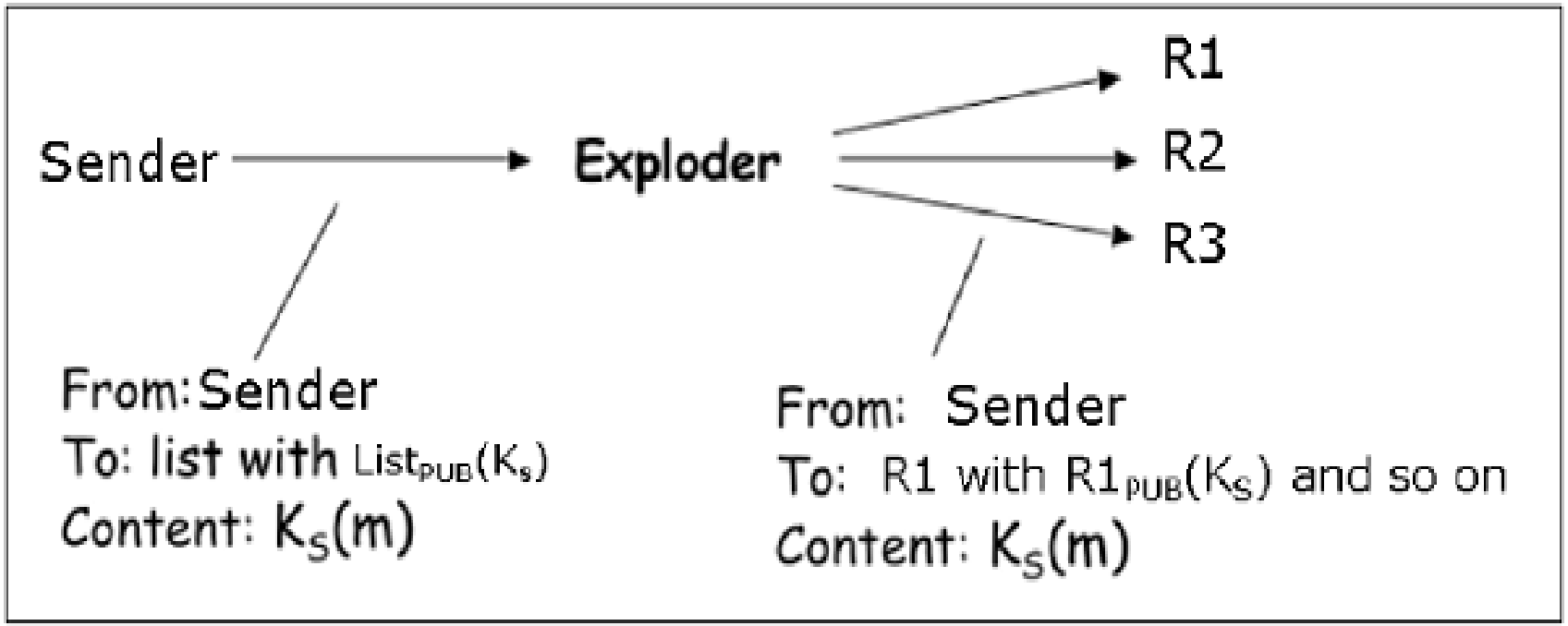
- Dịch vụ E-Mail Security (1-tới-nhiều)





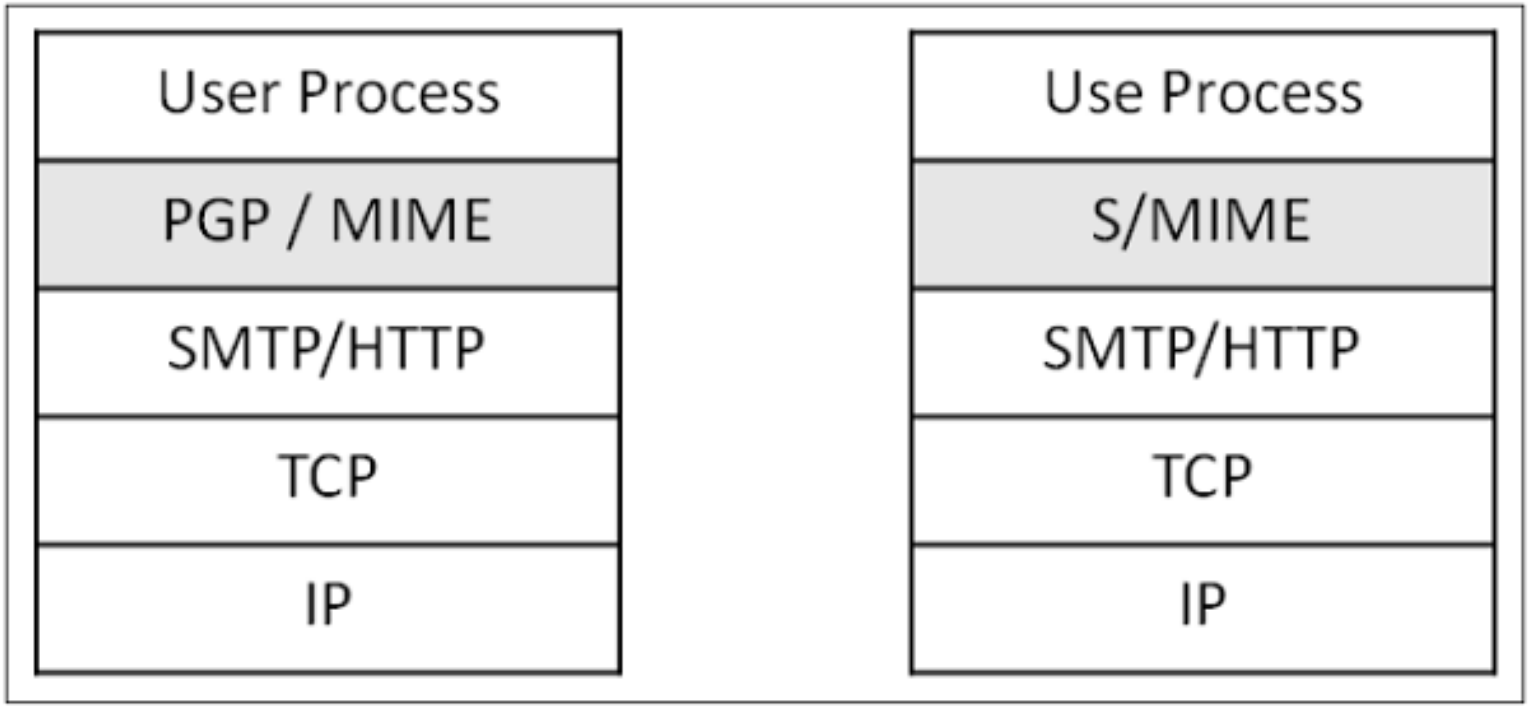
Giới thiệu

- Dịch vụ E-Mail Security (1-tới-nhiều)



Giới thiệu

- E-Mail Security với Pretty Good Privacy (PGP) hoặc Secure Multipurpose Internet Mail Extension (S/MIME)

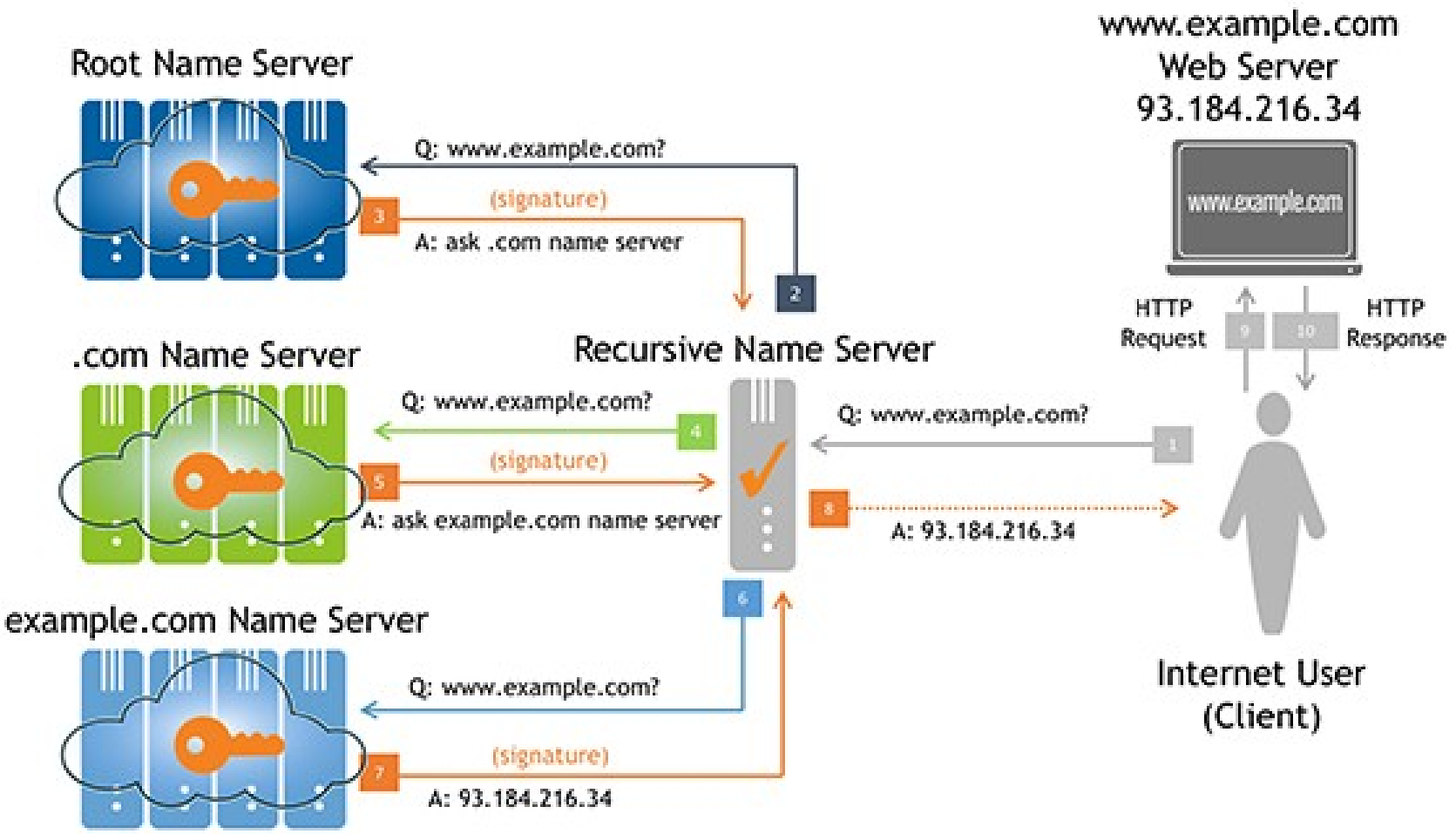


Giới thiệu

- DNS Security dựa trên mật mã khóa công khai
  - All information sent by a DNS server is signed with the originating zone's private key for ensuring authenticity. DNS clients need to know the zone's public keys to check the signatures. Clients may be preconfigured with the public keys of all the top-level domains, or root DNS.
  - Mọi vùng DNS đều có cặp khóa công khai/bí mật
  - Tất cả các thông tin được gửi bởi máy chủ DNS được ký kết với khóa bí mật của vùng gốc để đảm bảo tính xác thực
  - DNS khách cần biết khóa công khai của vùng để kiểm tra chữ ký
  - DNS khách có thể được cấu hình sẵn với các khóa công khai của tất cả các tên miền cấp cao nhất hoặc DNS gốc

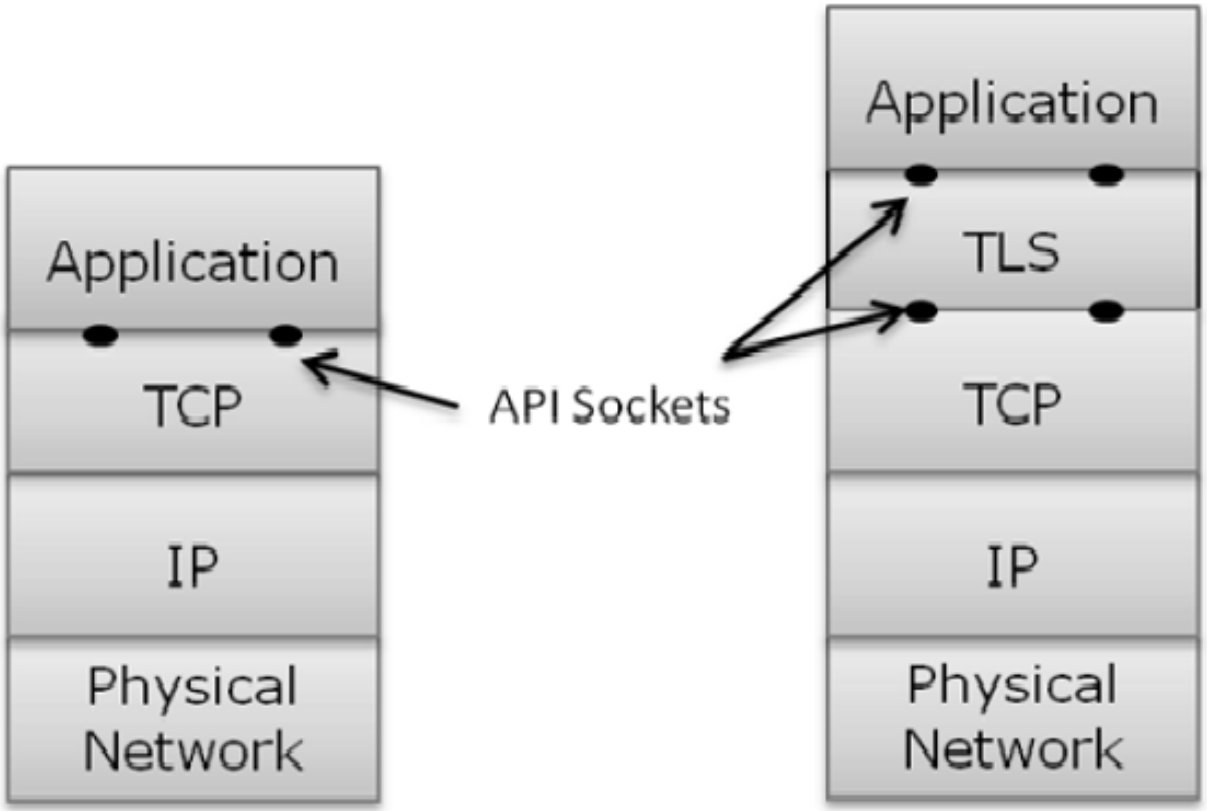
Giới thiệu

- DNS Security dựa trên mật mã khóa công khai



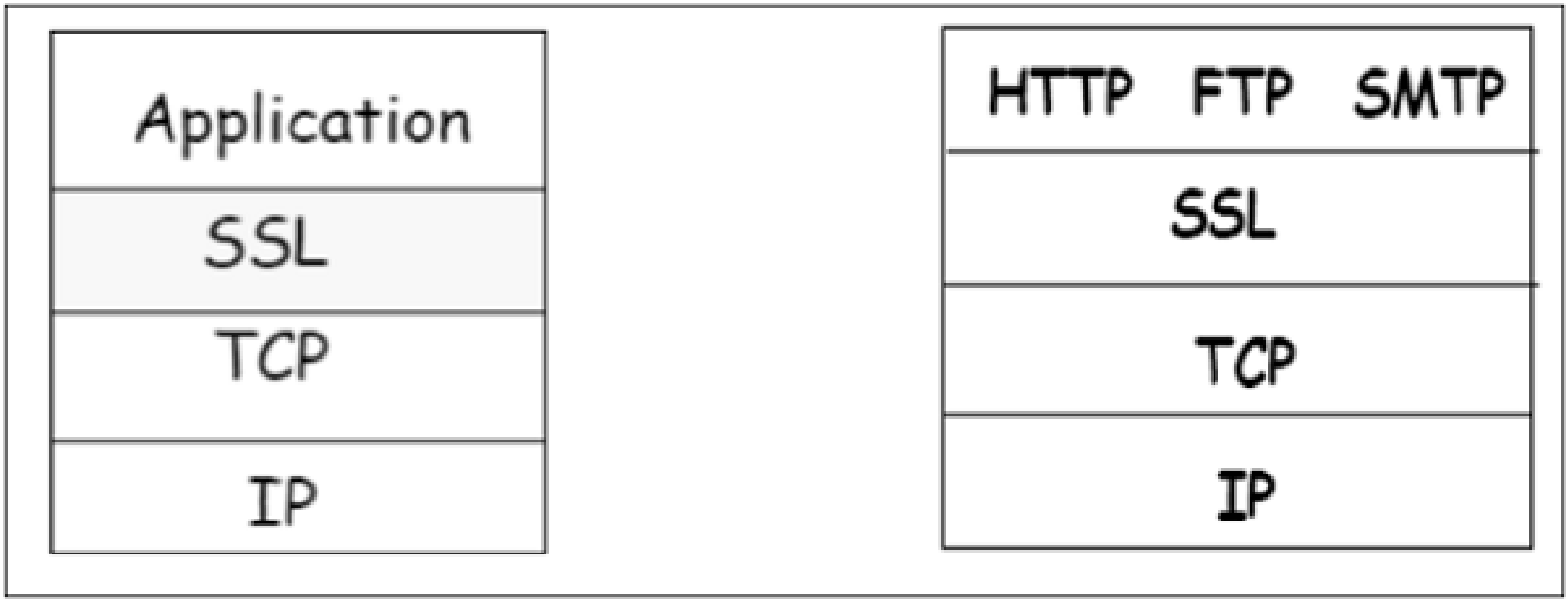
Giới thiệu

- Transport Layer Security (TLS)



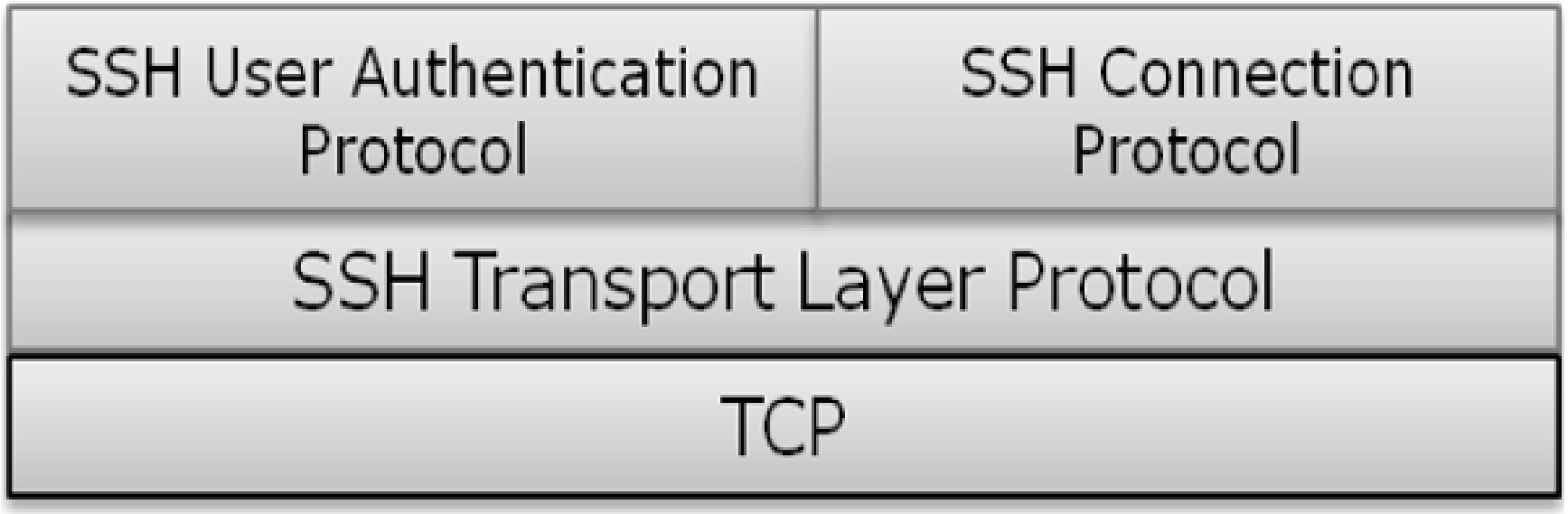
Giới thiệu

- Secure Socket Layer (SSL)



Giới thiệu

- Secure Shell Protocol (SSH)

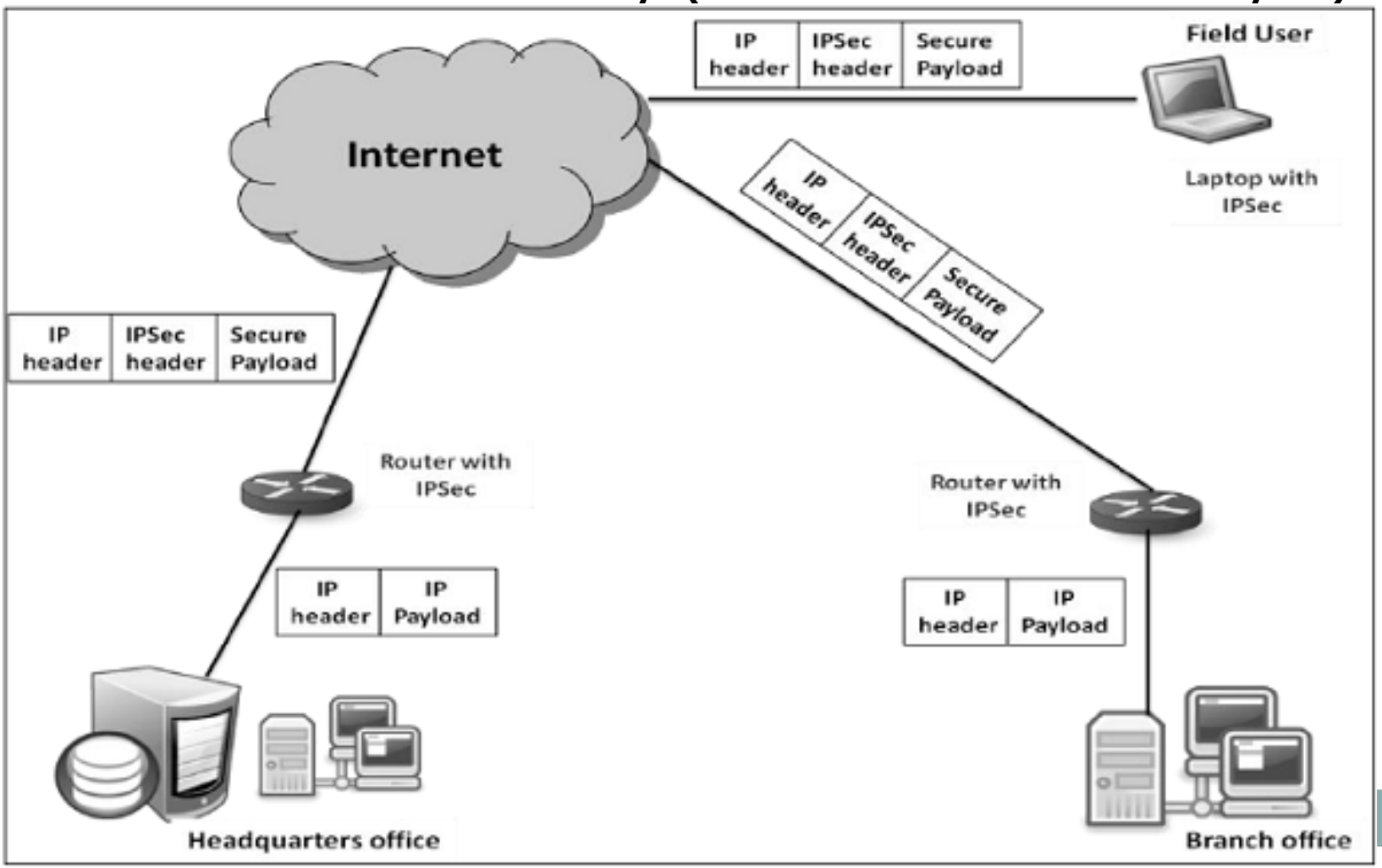


Giới thiệu

- Internet Protocol Security (IPSec in Network Layer)
  - Sử dụng cho Virtual Private Network (VPN), gateway-to-gateway, người dùng từ xa và mạng của tổ chức host-to-gateway
  - Thiết kế cho TCP, UDP, ICMP, etc.
  - Bảo vệ toàn bộ gói tin hiện diện ở lớp IP bao gồm các tiêu đề lớp cao hơn
  - Phần header của lớp cao hơn bao gồm số hiệu cổng được ẩn nên phân tích lưu lượng truyền tải khó hơn
  - Bảo mật: mã hóa gói tin, ngăn chặn nghe lén
  - Xác thực nguồn gốc gói tin nhận: nguồn trong header
  - Tính toàn vẹn: gói tin không bị thay đổi
  - Quản lý khóa: trao đổi khóa an toàn, chống lại tấn công

Giới thiệu

- Internet Protocol Security (IPSec in Network Layer)



Giới thiệu

- An ninh ở tầng Data Link (liên kết dữ liệu)
  - Phòng ngừa giả mạo ARP (Address Resolution Protocol ánh xạ địa chỉ IP với địa chỉ MAC): Static ARP, Intrusion Detection, Dynamic ARP Inspection
  - Phòng ngừa MAC Flooding (tấn công làm tràn switch với địa chỉ MAC sử dụng các gói ARP giả mạo), đánh cắp cổng (Port Stealing): intelligent Ethernet switches
  - Phòng ngừa tấn công DHCP (Dynamic Host Configuration Protocol): DHCP snooping
  - An ninh cho Wireless LAN: Wired Equivalent Privacy (WEP), 802.11i Protoco, WiFi Protected Access (WPA), WPA2

Giới thiệu

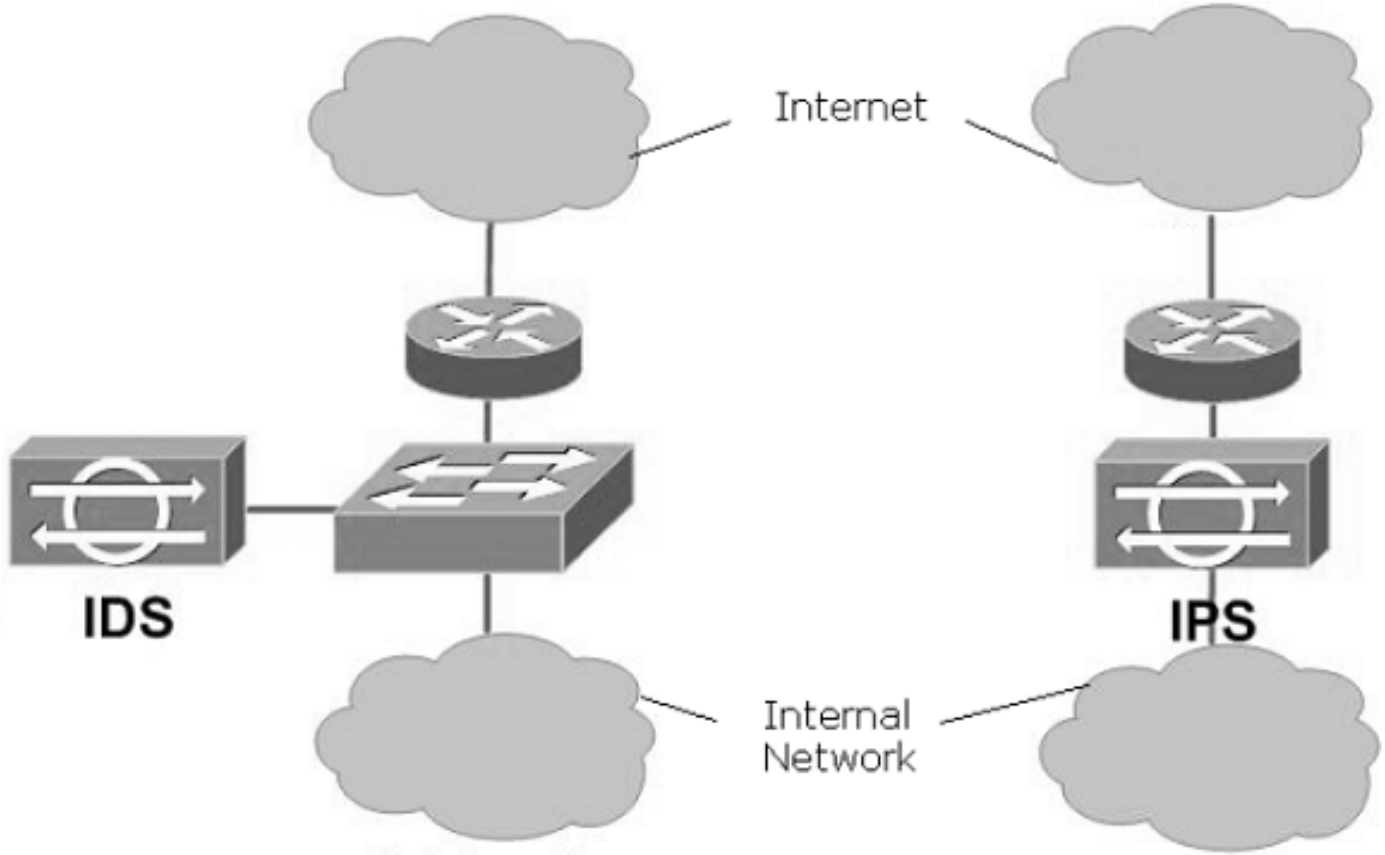
- Kiểm soát truy cập (Access Control)
  - Giới hạn quyền truy cập đến thiết bị mạng
  - Xác thực người dùng và ủy quyền
  - Xác thực bằng mật khẩu
  - Phương pháp xác thực tập trung
  - Danh sách kiểm soát truy cập

Giới thiệu

- Tường lửa (Firewall)
  - Có thể là một thiết bị phần cứng, phần mềm hoặc hệ thống kết hợp, ngăn chặn truy cập trái phép từ bên ngoài vào mạng nội bộ
  - Tất cả các gói dữ liệu vào/ra mạng nội bộ đi qua tường lửa, kiểm tra mỗi gói tin và chặn những gói không đáp ứng các tiêu chí an toàn đã được chỉ định
  - Ba kiểu tường lửa: Packet filter (Stateless & Stateful), Application-level gateway, Circuit-level gateway
  - Hệ thống phát hiện xâm nhập mạng (Intrusion Detection System, IDS)
  - Hệ thống chống xâm nhập mạng (Intrusion Prevention System, IPS)

Giới thiệu

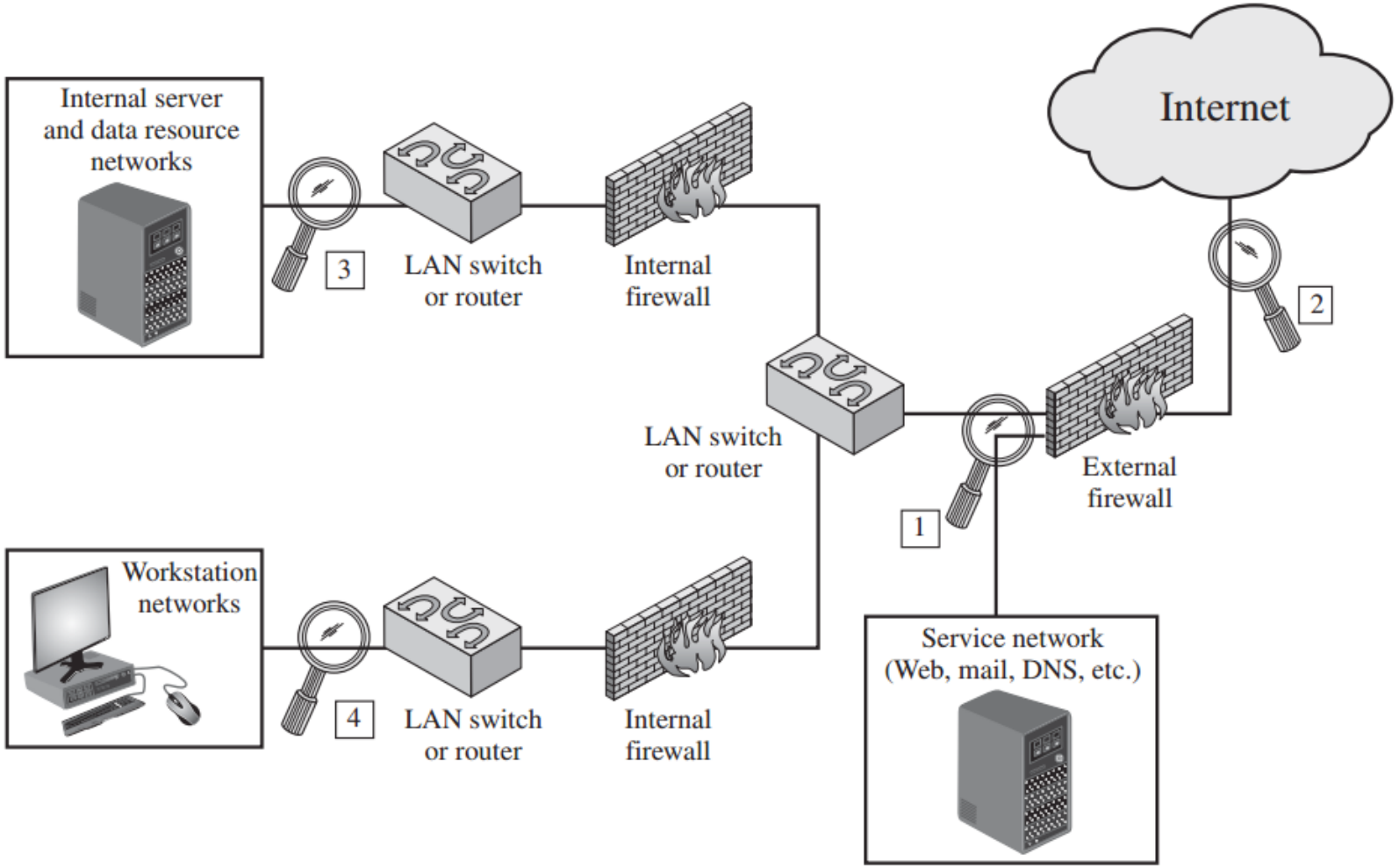
- Hệ thống phát hiện và chống xâm nhập mạng



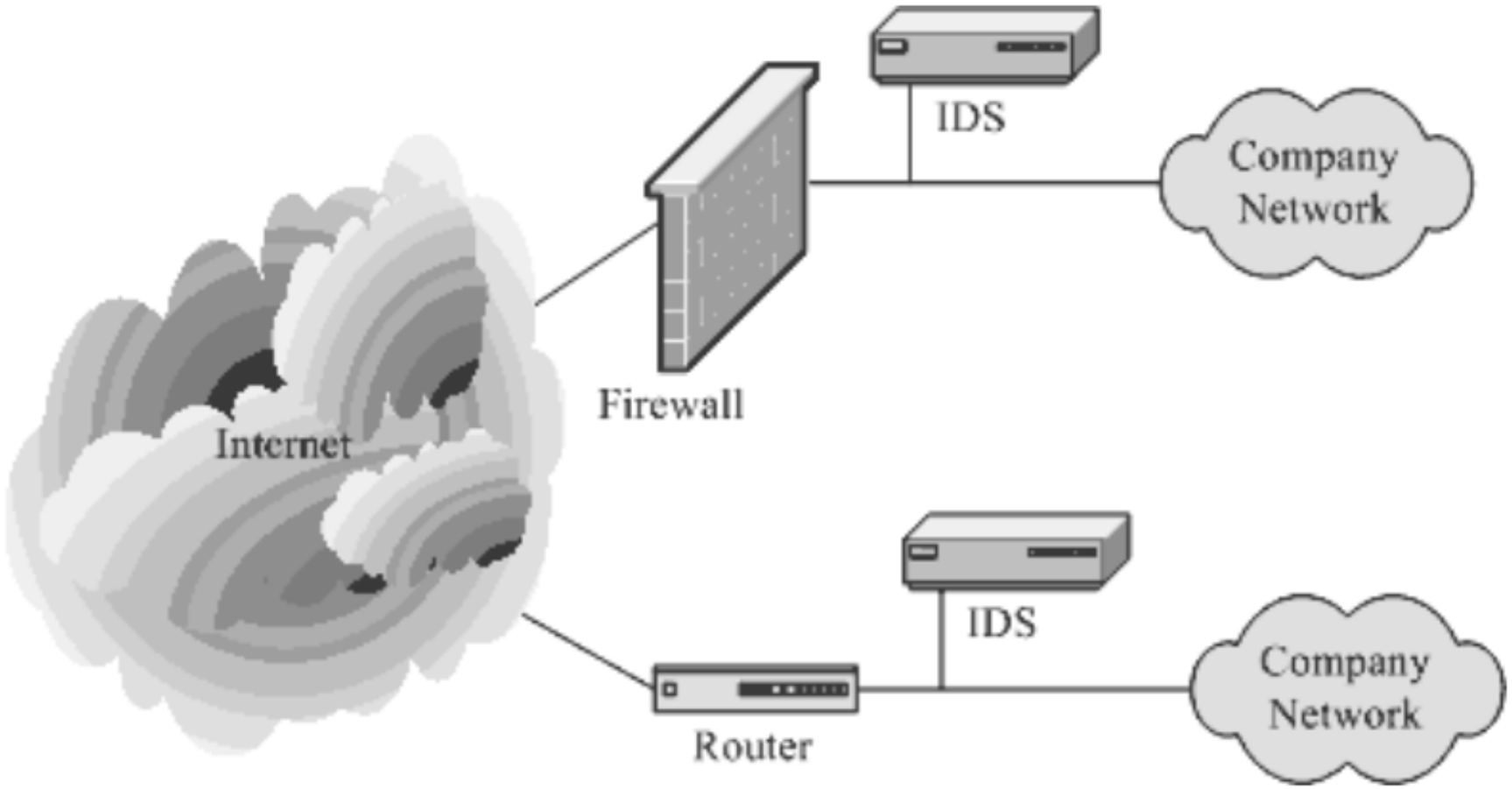
Nội dung

- Giới thiệu
- **Hệ thống phát hiện xâm nhập mạng**
- Phát hiện xâm nhập mạng với Snort
- Xây dựng luật cho Snort

Hệ thống phát hiện xâm nhập mạng



Hệ thống phát hiện xâm nhập mạng



Hệ thống phát hiện xâm nhập mạng

- Giám sát mọi hoạt động của hệ thống
  - Xác thực là hoạt động bình thường hay xâm nhập
  - Cảnh báo dựa vào dấu hiệu nhận dạng
  - Tầng ứng dụng: DHCP, DNS, Finger, FTP, HTTP, IMAP, IRC, NFS, POP, rlogin/rsh, RPC, SIP, SMB, SMTP, SNMP, Telnet, TFTP
  - Tầng vận chuyển: TCP, UDP
  - Tầng mạng: IPv4, ICMP

Hệ thống phát hiện xâm nhập mạng

- Giám sát mọi hoạt động của hệ thống
  - Có khi bị nhận dạng sai lầm
  - False Positive/Type I Error: hoạt động bình thường bị hệ thống IDS nhận dạng là xâm nhập
  - False Negative/Type II Error: xâm nhập mạng nhưng hệ thống IDS không phát hiện được

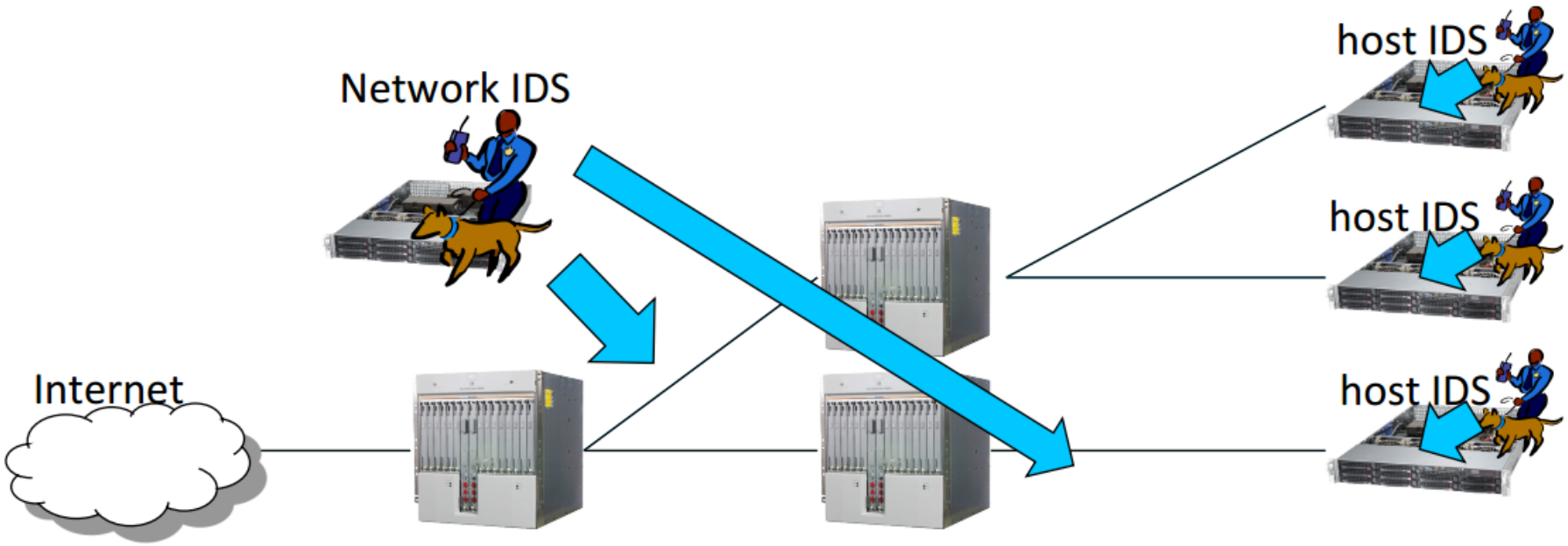
Hệ thống phát hiện xâm nhập mạng

- Phát hiện xâm nhập dựa vào dấu hiệu nhận dạng
  - Cơ sở dữ liệu chứa các xâm nhập đã biết với dấu hiệu nhận dạng
  - Dấu hiệu nhận dạng: kiểu, thứ tự của các gói mô tả một xâm nhập cụ thể
  - Chỉ nhận dạng được các xâm nhập đã biết
- Phát hiện xâm nhập dựa vào dấu hiệu bất thường
  - Tạo các mẫu của tác vụ bình thường của mạng
  - Phát hiện dấu hiệu bất thường (khác với tác vụ bình thường)

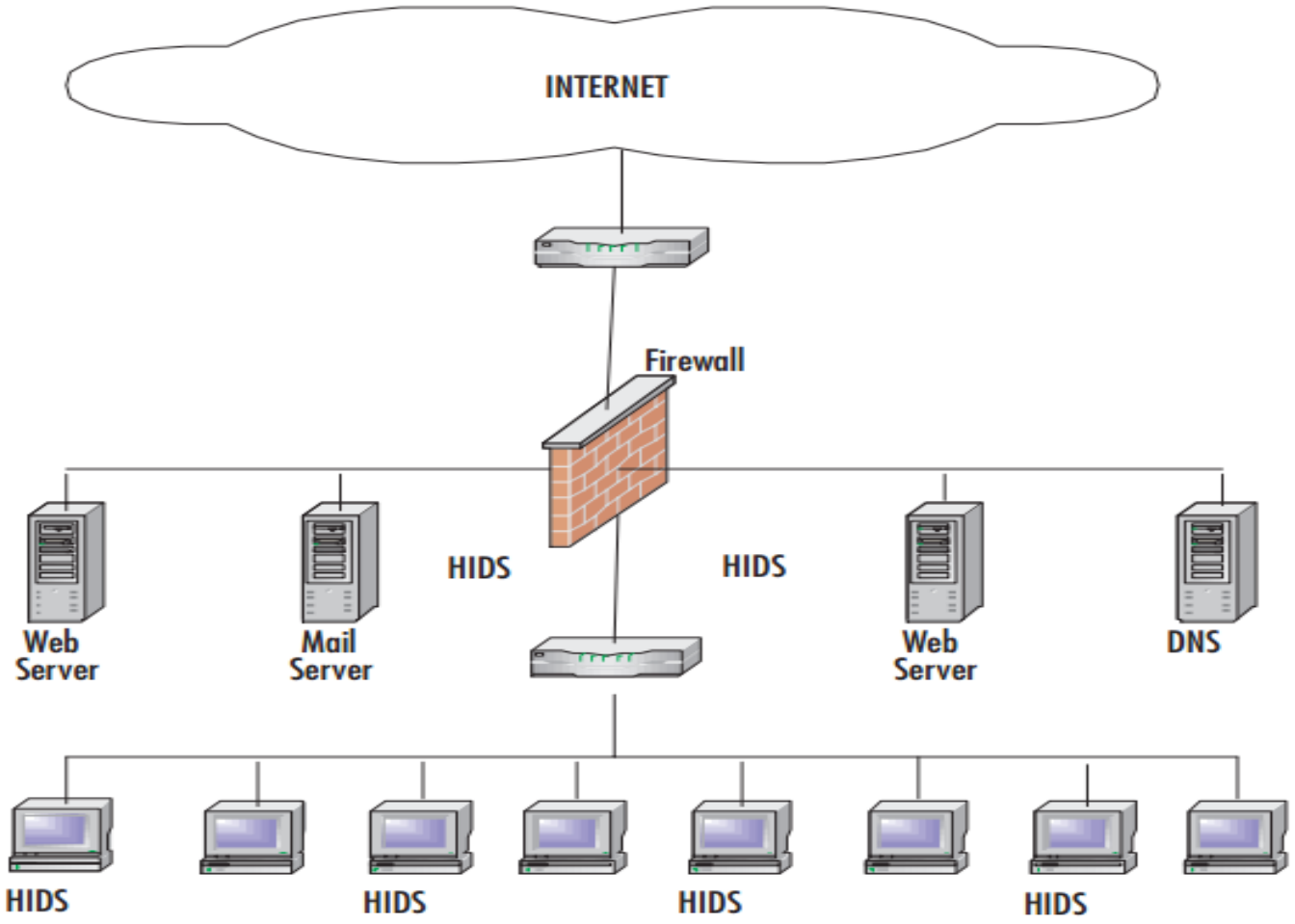
Hệ thống phát hiện xâm nhập mạng

- Host-Based IDS
  - Quét log file, mở kết nối mạng, quét đĩa, cảnh báo khi phát hiện xâm nhập
  - Phân tích log file, đĩa
- Network-based IDS
  - Giám sát thông tin được truyền tải trên mạng, cảnh báo khi phát hiện xâm nhập
  - Phân tích thông tin được truyền tải trên mạng

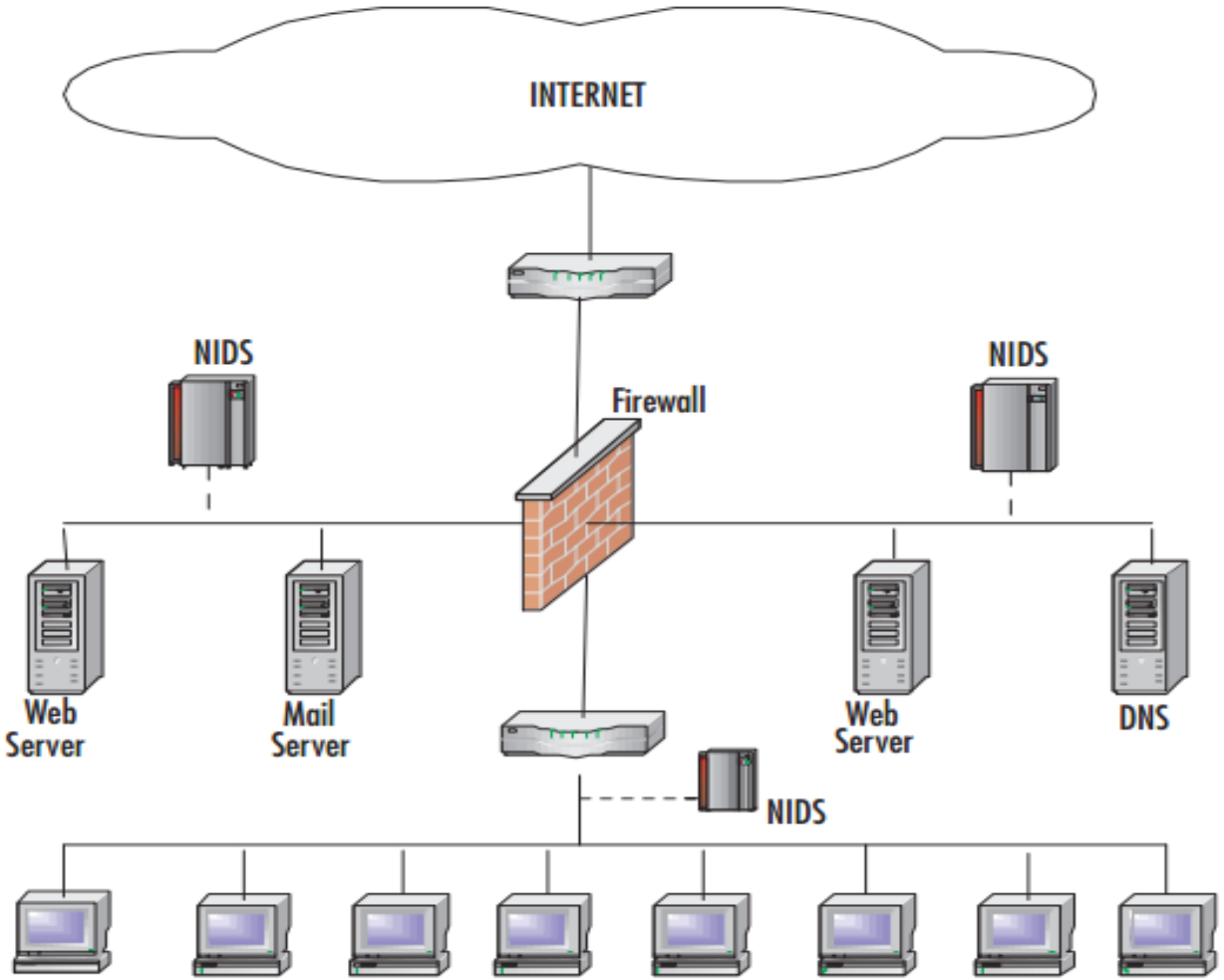
Hệ thống phát hiện xâm nhập mạng



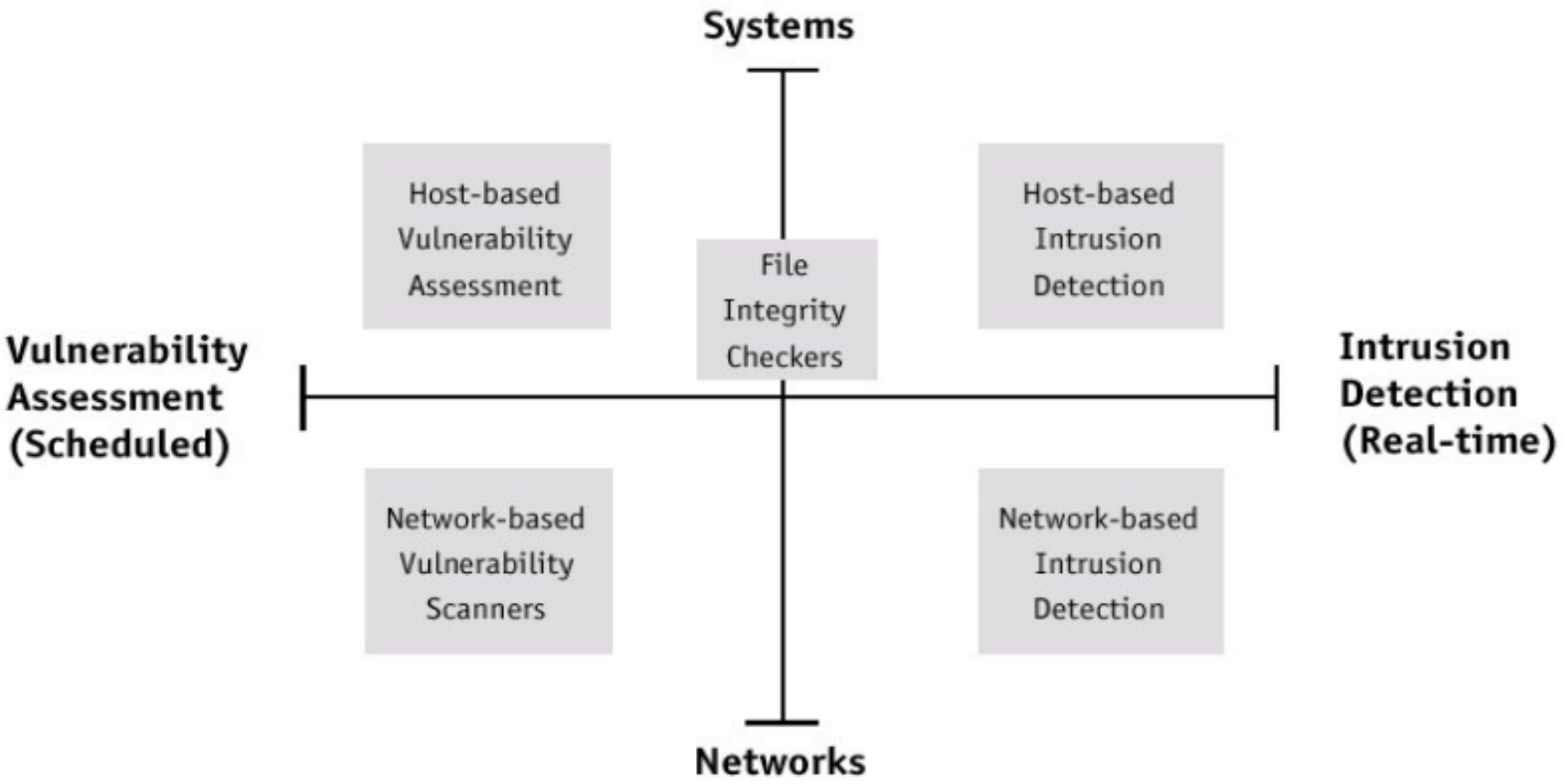
Hệ thống phát hiện xâm nhập mạng



Hệ thống phát hiện xâm nhập mạng



Hệ thống phát hiện xâm nhập mạng



Nội dung

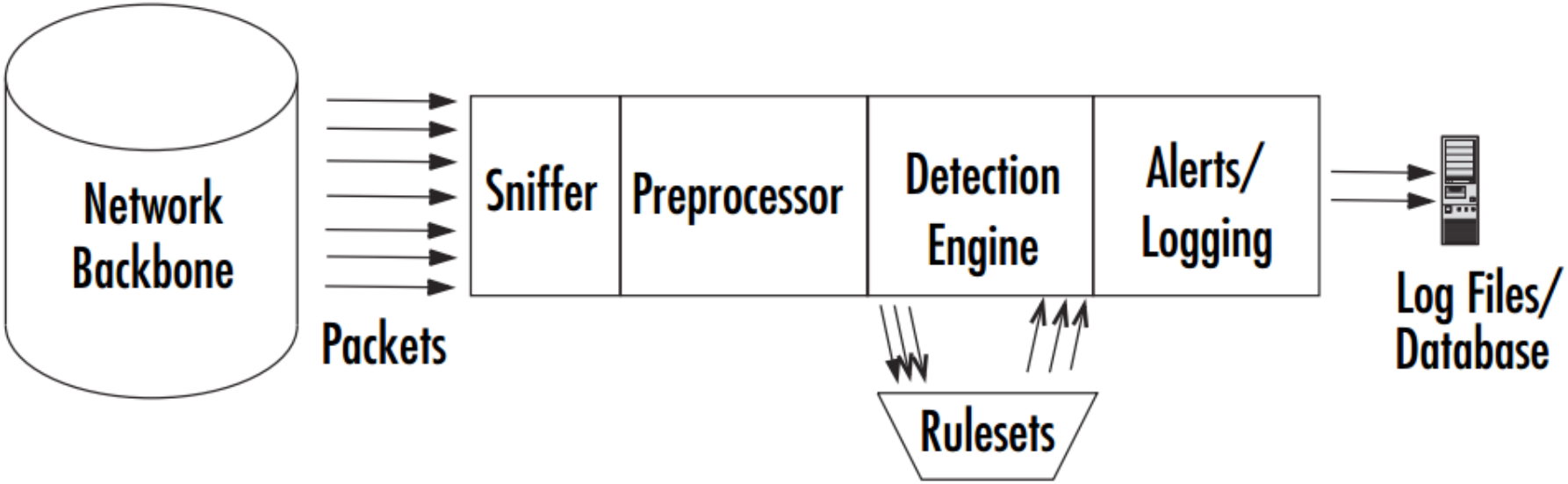
- Giới thiệu
- Hệ thống phát hiện xâm nhập mạng
- **Phát hiện xâm nhập mạng với Snort**
- Xây dựng luật cho Snort

Phát hiện xâm nhập mạng với SNORT

- Snort
  - Hệ thống phần mềm nguồn mở cho phát hiện và chống xâm nhập mạng, được tạo ra bởi Martin Roesch năm 1998, Sourcefire, sở hữu bởi Cisco từ năm 2013
  - Có khả năng phân tích thời gian thực gói tin được truyền tải trên mạng, ghi nhận nhật ký
  - 5 triệu lượt tải về và 600K người đăng ký sử dụng
  - Cộng đồng thường xuyên cập nhật tập luật

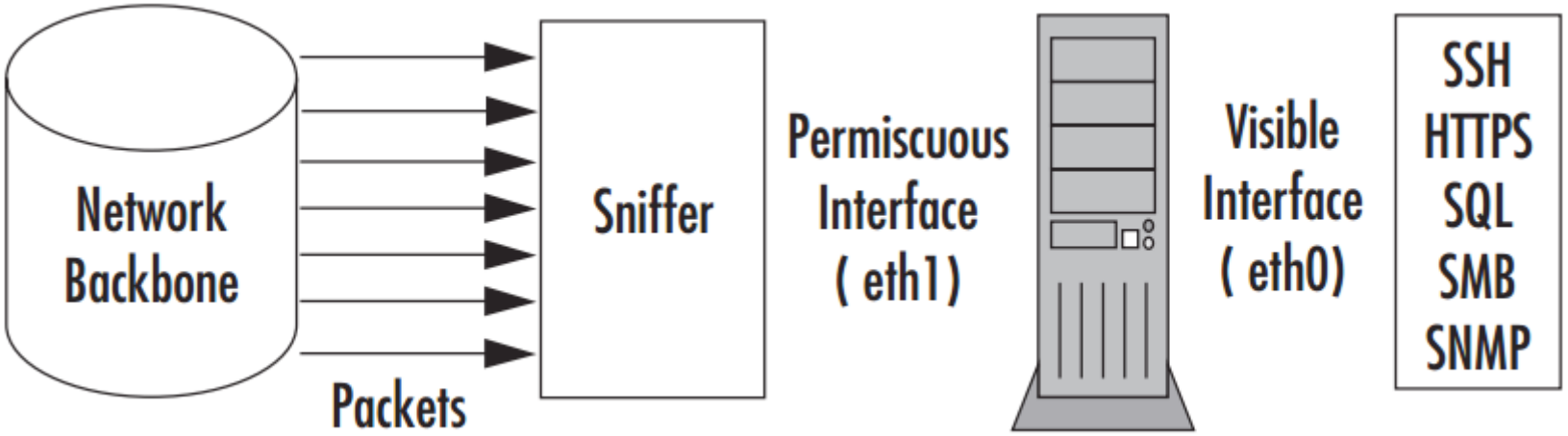
Phát hiện xâm nhập mạng với SNORT

- Kiến trúc Snort



Phát hiện xâm nhập mạng với SNORT

- Packet-Sniffing: thu thập thông tin để xem xét và xử lý

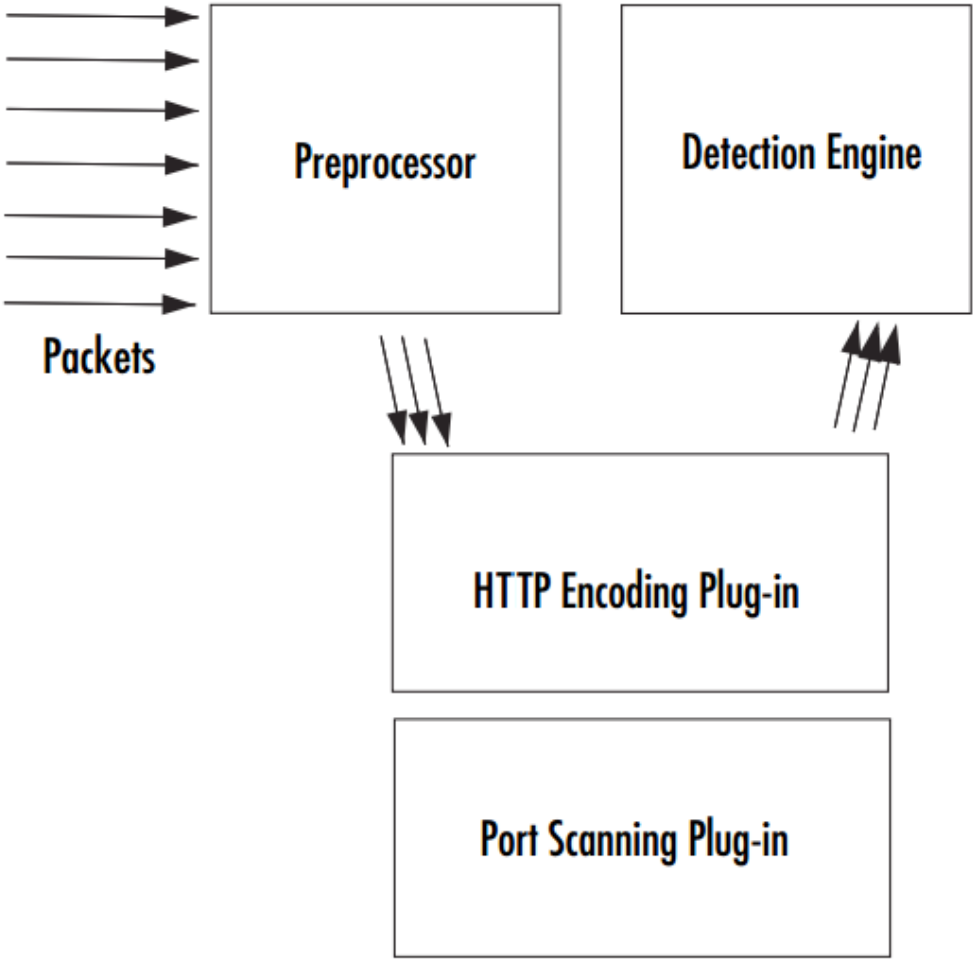


Phát hiện xâm nhập mạng với SNORT

- Preprocessor
  - Nhận gói tin thô và kiểm tra chúng có cắm vào RPC, HTTP, quét dò cổng (port scanner), phân mảnh IP (IP fragmentation handling), kiểm soát lưu lượng (flow control)
  - Sau khi đã xác định được kiểu hành vi của gói tin, bộ tiền xử lý sẽ gửi đến bộ phận phát hiện (detection engine)

Phát hiện xâm nhập mạng với SNORT

- Preprocessor

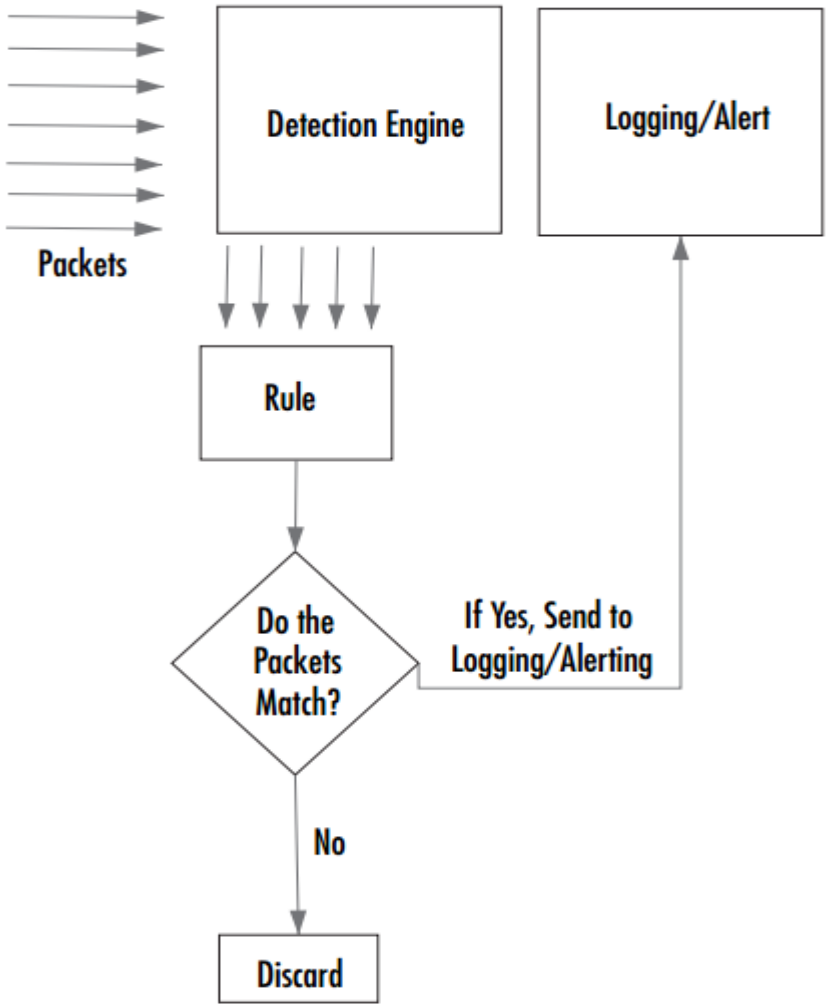


Phát hiện xâm nhập mạng với SNORT

- Detection Engine
  - Phát hiện xâm nhập dựa vào các dấu hiệu nhận dạng
  - Nhận gói tin từ bộ tiền xử lý, kiểm tra các dấu hiệu nhận dạng được mô tả trong tập luật, nếu khớp với dấu hiệu nhận dạng thì sẽ gửi đến bộ cảnh báo (alert processor)
  - Tập luật bao gồm 3 loại: Trojan horses, buffer overflows, truy xuất đến các ứng dụng
  - Luật: header và option
  - Header: hành động (alert/log), kiểu gói tin (TCP, UDP, ICMP, etc), địa chỉ và cổng nguồn, đích
  - Option: chứa dấu hiệu nhận dạng

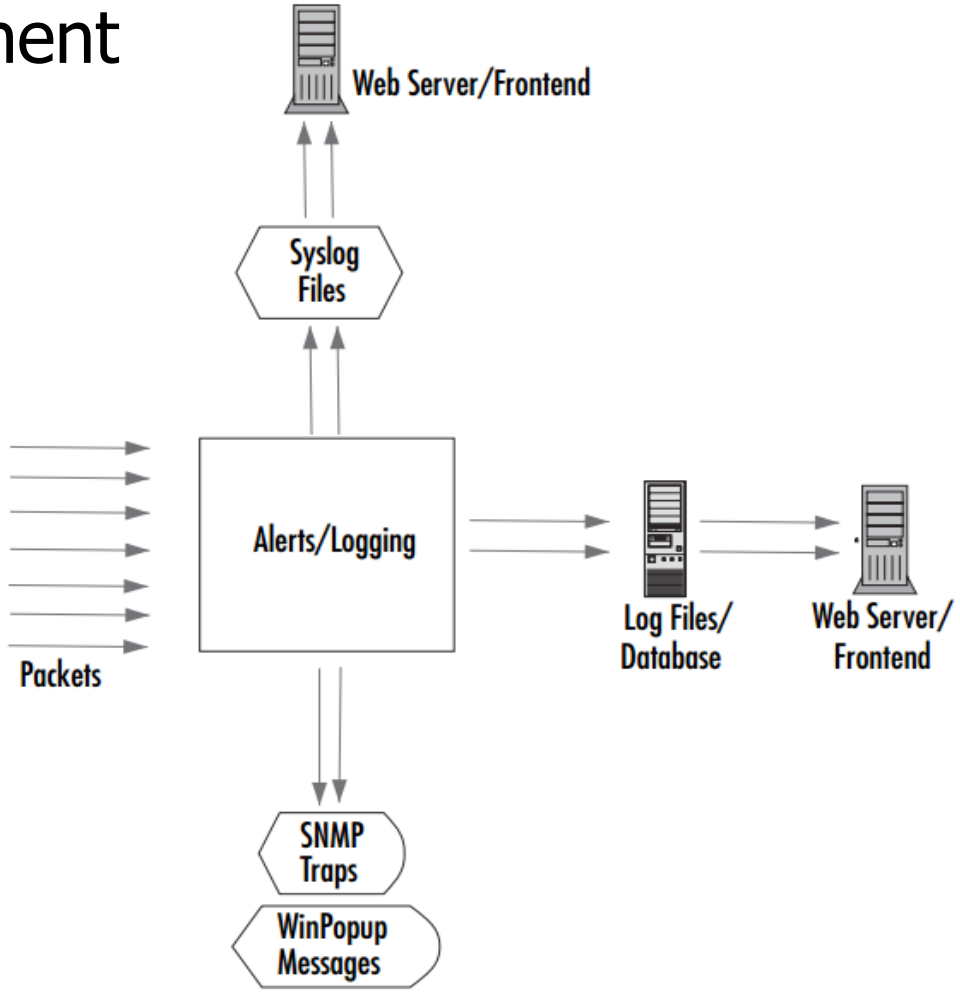
Phát hiện xâm nhập mạng với SNORT

- Detection Engine



Phát hiện xâm nhập mạng với SNORT

- Alerting/Logging Component



Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - sudo apt-get update
  - sudo apt-get install flex bison build-essential checkinstall libpcap-dev libnet1-dev libpcre3-dev libmysqlclient15-dev libpcap-dev libnet1-dev libpcre3-dev libmysqlclient15-dev libnetfilter-queue-dev iptables-dev
  - sudo apt-get install -y autoconf libtool pkg-config

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - mkdir inst
  - cd inst/
  - wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
  - wget https://www.snort.org/downloads/snort/snort-2.9.11.tar.gz
  - wget https://github.com/nghttp2/nghttp2/releases/download/v1.17.0/nghttp2-1.17.0.tar.gz

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - tar -xzvf nghttp2-1.17.0.tar.gz
  - cd nghttp2-1.17.0
  - autoreconf -i --force
  - automake
  - autoconf
  - ./configure --enable-lib-only
  - make
  - sudo make install
  - sudo ldconfig

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - tar -xvzf daq-2.0.6.tar.gz
  - cd daq-2.0.6
  - ./configure
  - make
  - sudo make install
  - sudo ldconfig

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - tar -zxvf snort-2.9.11.tar.gz
  - cd snort-2.9.11/
  - ./configure
  - make
  - sudo make install
  - sudo ldconfig
  - snort -V

    Version 2.9.11 GRE (Build 125)

    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team

    Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.

    …

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - sudo groupadd snort
  - sudo useradd snort -d /var/log/snort -s /sbin/nologin -c SNORT_IDS -g snort
  - sudo mkdir /var/log/snort
  - sudo chown snort:snort /var/log/snort
  - sudo mkdir /etc/snort

  - download snortrules-snapshot-29110.tar.gz
  - sudo tar zxvf snortrules-snapshot-29110.tar.gz -C /etc/snort/
  - sudo touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
  - sudo mkdir /usr/local/lib/snort_dynamicrules
  - sudo mv /etc/snort/etc/* /etc/snort/
  - sudo chown -R snort:snort /etc/snort/*

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04

```
/etc/snort
├── attribute_table.dtd
├── classification.config
├── file_magic.conf
├── gen-msg.map
├── preproc_rules
├── reference.config
├── rules
..  ├── local.rules
..  ├── black_list.rules
    ├── white_list.rules
     ..
├── sid-msg.map
├── snort.conf
├── so_rules
├── threshold.conf
└── unicode.map
```

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf
  - sudo nano /etc/snort/snort.conf

    ################## EDIT CONFIG /etc/snort/snort.conf

    ipvar HOME_NET 192.168.8.0/24

    ipvar EXTERNAL_NET !$HOME_NET

    var RULE_PATH /etc/snort/rules

    var SO_RULE_PATH /etc/snort/so_rules

    var PREPROC_RULE_PATH /etc/snort/preproc_rules

    var WHITE_LIST_PATH /etc/snort/rules

    var BLACK_LIST_PATH /etc/snort/rules

    #removing the ‘lzma’ keyword

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - sudo snort -T -i eth0 -u snort -g snort -c /etc/snort/snort.conf

```
        --== Initialization Complete ==--
 ,,_     -*> Snort! <*-
o"  )~   Version 2.9.11 GRE (Build 125)
 ""      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
         Copyright (C) 2014-2017 Cisco and/or its affiliates. All rights reserved.
         Copyright (C) 1998-2013 Sourcefire, Inc., et al.
         Using libpcap version 1.5.3
         Using PCRE version: 8.31 2012-07-06
         Using ZLIB version: 1.2.8
...
Snort successfully validated the configuration!
Snort exiting
```

Phát hiện xâm nhập mạng với SNORT

- Cài đặt Snort 2.9.11 trên Ubuntu 14.04
  - sudo nano /etc/snort/rules/local.rules

    alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)
  - sudo snort -T -c /etc/snort/snort.conf -i eth0
  - sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0
  - Khi có máy tính sử dụng lệnh ping đến địa chỉ IP của giao diện eth0 máy snort, màn hình máy snort hiển thị như sau:

    … [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] …

    … [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] …

    … [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] …

    … [**] [1:10000001:1] ICMP test detected [**] [Classification: Generic ICMP event] …

    …

Nội dung

- Giới thiệu
- Hệ thống phát hiện xâm nhập mạng
- Phát hiện xâm nhập mạng với Snort
- **Xây dựng luật cho Snort**

Viết luật cho SNORT

- Định dạng luật Snort: **Header** + **Options**
- Header: hành động, nghi thức, địa chỉ IP và cổng nguồn, đích (có thể sử dụng netmask)
- Options: thông báo cảnh báo, mô tả dấu hiệu nhận dạng, phân loại, etc.
- Ví dụ luật Snort
  - alert icmp any any -> $HOME_NET any (msg:"ICMP test detected"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

Viết luật cho SNORT

Header Format						
Action	Proto	SRC	SRC Port	Direction	DST	DST Port

Action	Function
alert	alerts and logs event
log	logs event
pass	ignores event
drop	drops packet and logs event
reject	TCP reset of session or ICMP Type3 Code 3 of UDP traffic and logs
sdrop	drops packet without logging
activate	drops packet without logging
dynamic	alerts and activates a dynamic rule

Proto
IP (covers all)
TCP
UDP
ICMP

Direction	Meaning
->	from SRC to DEST
<>	in either direction

Source/Destination Port	Meaning
A.B.C.D	Single IPA
A.B.C.D/XX	CIDR
[A.B.C.D, A.B.C.E, A.B.C.G]	Match ANY, not all

Viết luật cho SNORT

Modifier	Function
nocase;	makes previous content match case insensitive, should be used in most cases to allow for vendor implementation variations. Should NOT be used when trying to match Base64 or URL encoding.
rawbytes;	ignores pre--processor interpretation of payload contents and looks for a raw packet payload match
offset:	advances pointer to after a number of bytes from the beginning of the PAYLOAD. Example offset:3;
depth:	will only look for the content match from the beginning of the PAYLOAD up to the specified byte number.
distance:	advances the pointer to after the number of bytes from the end of the last CONTENT MATCH Example distance:12;
within:	will only look for the content match from the end of the last CONTENT MATCH through the specified number of bytes

Viết luật cho SNORT

- Ví dụ
  - alert tcp any any -> any 21 (msg:"FTP ROOT"; content:"USER root"; nocase;)
  - alert tcp any any -> any 21 (msg:"Telnet NOP"; content:"|FF F1|"; rawbytes;)
  - alert tcp any any -> any 80 (content:"cgi-bin/phf"; offset:4; depth:20;)
  - alert tcp any any -> any any (content:"ABC"; content:"DEF"; distance:1;)
  - alert tcp any any -> any any (content:"ABC"; content:"EFG"; within:10;)

Viết luật cho SNORT

Basic Body Options	
Operator	**Options**
msg:	ascii text to be printed in alert or log, must be in quotes eg msg:"Yet another Scan";
reference:	will call a link to specific documentation of rules included in snort rule set (100--999,999) example reference:cve,CVE--1999--0105;
sid:	Snort ID number, <100 reserved, 100---1000000 (now 2000000) used for packaged rules, above that are custom
rev:	revision of the snort rule (or set)
classtype:	a named class of attack, built in ones are associated with a certain priority. Example classtype:attempted_recon;
priority:	level of concern, 1 is really bad, 2 not so bad, 3 informational, etc.
content:	searches the entire packet payload for either an ASCII string or a "binary" match.

Viết luật cho SNORT

- Reference

System	URL Prefix
bugtraq	http://www.securityfocus.com/bid/
cve	http://cve.mitre.org/cgi-bin/cvename.cgi?name=
nessus	http://cgi.nessus.org/plugins/dump.php3?id=
arachnids	(currently down) http://www.whitehats.com/info/IDS
mcafee	http://vil.nai.com/vil/content/v_
osvdb	http://osvdb.org/show/osvdb/
msb	http://technet.microsoft.com/en-us/security/bulletin/
url	http://

- Ví dụ
  - alert tcp any any -> any 7070 (msg:"IDS411/dos-realaudio"; flags:AP; content:"|fff4 fffd 06|"; reference:arachnids,IDS411;)

Viết luật cho SNORT

Classtype	Description	Priority
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
successful-user	Successful User Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
unsuccessful-user	Unsuccessful User Privilege Gain	high
web-application-attack	Web Application Attack	high
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
bad-unknown	Potentially Bad Traffic	medium
default-login-attempt	Attempt to login by a default username and password	medium
denial-of-service	Detection of a Denial of Service Attack	medium

Viết luật cho SNORT

Classtype	Description	Priority
misc-attack	Misc Attack	medium
non-standard-protocol	Detection of a non-standard protocol or event	medium
rpc-portmap-decode	Decode of an RPC Query	medium
successful-dos	Denial of Service	medium
successful-recon-largescale	Large Scale Information Leak	medium
successful-recon-limited	Information Leak	medium
suspicious-filename-detect	A suspicious filename was detected	medium
suspicious-login	An attempted login using a suspicious user-name was detected	medium
system-call-detect	A system call was detected	medium
unusual-client-port-connection	A client was using an unusual port	medium
web-application-activity	Access to a potentially vulnerable web appli-cation	medium
icmp-event	Generic ICMP event	low
misc-activity	Misc activity	low

Viết luật cho SNORT

Classtype	Description	Priority
network-scan	Detection of a Network Scan	low
not-suspicious	Not Suspicious Traffic	low
protocol-command-decode	Generic Protocol Command Decode	low
string-detect	A suspicious string was detected	low
unknown	Unknown Traffic	low
tcp-connection	A TCP connection was detected	very low

- Ví dụ
  - alert tcp any any -> any 7070 (msg:"IDS411/dos-realaudio"; flags:AP; content:"|fff4 fffd 06|"; reference:arachnids,IDS411;)

Viết luật cho SNORT

Basic Body Options	
Operator	**Options**
isdataat:	Verifies a certain number of bytes is present, can be made relative to previous content by adding relative to the end
uricontent:	Same as content, but applies specifically to uri's
urilen:	Specifies a particular length of URI, or range of lengths. Requires HTTP Pre--processor
flow:	describes state of session and directionality. Includes options: to_server from_server, to_client from_client only_stream no_stream stateless established
ipopts:	indicates the presence of options fields in the IP header . Includes: eol-- End of List lsrr --Loose Source Routing rr –Record Route satid – Stream ID sec – Security ssrr – Strict Source Routing ts – Time Stamp
dsize:	indicates a size, or size range of the entire packet (includes headers)

Viết luật cho SNORT

- Ví dụ
  - alert tcp any any -> 192.168.1.1 80 (sid:1002354;rev:2;msg:"Warning!!, A host is trying to access /admin"; uricontent:"/admin";classtype:web-application-activity;)
  - alert tcp any any -> any 111 (content:"PASS"; isdataat:50,relative; content:!"|0a|"; within:50;)
  - alert ip any any -> 192.168.1.0/24 any (dsize: > 6000; msg: "Large size IP packet detected";)
  - alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (flow:to_server,established;)
  - alert ip any any -> $HOME_NET any (ipopts: lsrr; msg: “Loose source routing attempt”; sid: 1000001;)

Viết luật cho SNORT

Basic Body Options	
Operator	**Options**
flags:	indicates the presence of TCP Flags. Includes: A – Ack F – Fin P – Push Snort Cheat Sheet R – Reset S – Syn U – Urgent Data 0 – No Flags (used in nmap null scan) 1 – Reserved bit 1 (ECN) 2 – Reserved bit 2 (CWR) + -- Multiple Flags * -- Any Flag ! – Not that flag
ttl:	specifies a particular time to live value in the IP header, some decimal number between 0-- 255.
tag:	used to log a series of packets rather than just one. Think of it as a trigger. Tag largely replaces the activate: à? dynamic: pair. Parameters: session – logs all packets in the session that triggered the rule host – logs all packets to/from host who's IP triggered the rule (this will capture all traffic, not just that particular session – good for capturing botnet activity) count – how much to log, a decimal number packets – logs that many packets seconds – logs all packets for the session or host for a specified number of seconds SRC – only logs packets from source DST – only logs packets from destination

Viết luật cho SNORT

- Ví dụ
  - alert tcp any any -> any any (flags: SF; msg: “SYNC-FIN packet detected”;)
  - alert icmp any any -> 192.168.1.0/24 any (msg: "Ping with TTL=100"; ttl:100;)
  - alert tcp any any -> any 23 (flags:S,CE; tag:session,10,seconds;)
  - alert tcp $EXTERNAL_NET any -> 192.168.1.0/24 80 (msg:”Sample alert”; pcre:”/GET.*\.htm/i”; classtype: webapplication-activity; reference:url, http://www.abc.com/20180405.html; sid:20180405; rev:1;)

Viết luật cho SNORT

- Ví dụ
  - alert icmp any any -> any any (dsize: > 10000 msg: “Ping of Death Detected”; sid:777777)
  - alert tcp any any -> 192.168.1.1 any (msg:"TCP SYN Flooding attack detected"; flags:S; threshold: type threshold, track by_dst, count 10 , seconds 30; sid: 5000001; rev:1;)
  - alert tcp $external_net any -> $http_servers $http_ports (msg:"web-misc robots.txt access"; flow:to_server, established; uricontent:"/robots.txt"; nocase; reference:nessus,10302; classtype:web-application-activity; threshold:type threshold, track by_dst, count 10 , seconds 60 ; sid:1000852; rev:1;)