Mục 4.1: Điều khiển truy cập

1. Điều khiển truy nhập là gì?

a) Quá trình chỉ xác thực người dùng.

b) Quá trình chỉ trao quyền cho người dùng.

c) Quá trình nhận dạng, trao quyền truy nhập thông tin, hệ thống, tài nguyên cho người dùng.

d) Quá trình chỉ quản trị tài khoản người dùng.

2. Mục đích chính của điều khiển truy nhập KHÔNG bao gồm yếu tố nào sau đây?

a) Tính bí mật (Confidentiality)

b) Tính toàn vẹn (Integrity)

c) Tính sẵn dùng (Availability)

d) Tính ẩn danh (Anonymity)

3. Xác thực (Authentication) trong điều khiển truy nhập là gì?

a) Quá trình xác minh tính chân thực của thông tin nhận dạng người dùng cung cấp.

b) Quá trình xác định tài nguyên người dùng được phép truy nhập.

c) Quá trình thêm, bớt, sửa đổi tài khoản người dùng.

d) Quá trình cấp quyền truy nhập dựa trên vai trò.

4. Đâu là một ví dụ về biện pháp điều khiển truy nhập tuỳ chọn (DAC)?

a) Hệ thống phân loại tài liệu theo mức độ Mật, Tối mật.

b) Người dùng chia sẻ file trong thư mục cá nhân của mình cho người khác.

c) Nhân viên ngân hàng chỉ truy cập được dữ liệu khách hàng theo chức vụ.

d) Firewall chặn truy cập dựa trên địa chỉ IP.

5. Trong điều khiển truy nhập bắt buộc (MAC), quyền truy nhập được xác định dựa trên yếu tố nào?

a) Quyết định của chủ sở hữu tài nguyên.

b) Vai trò của người dùng trong tổ chức.

c) Tính nhạy cảm của thông tin và sự trao quyền chính thức.

d) Các luật được định nghĩa trước bởi quản trị viên.

6. Công nghệ điều khiển truy nhập nào sử dụng "cái bạn có" và "cái bạn biết" để xác thực?

a) Điều khiển truy nhập dựa trên mật khẩu.

b) Điều khiển truy nhập dựa trên đặc điểm sinh trắc học.

c) Điều khiển truy nhập dựa trên thẻ thông minh (Smartcard).

d) Điều khiển truy nhập dựa trên khóa mã (Encrypted Keys).

7. Mật khẩu một lần (OTP) là gì?

a) Mật khẩu người dùng tự đặt và không bao giờ thay đổi.

b) Mật khẩu được sinh ra và chỉ được dùng 1 lần cho 1 phiên làm việc hoặc giao dịch.

c) Mật khẩu được mã hóa bằng thuật toán MD5.

d) Mật khẩu có độ dài tối thiểu 8 ký tự.

8. Đâu KHÔNG phải là một đặc điểm sinh trắc học thường dùng để điều khiển truy nhập?

a) Dấu vân tay

b) Khuôn mặt

c) Giọng nói

d) Nhóm máu

9. Sự khác biệt cơ bản giữa DAC (Điều khiển truy nhập tuỳ chọn) và MAC (Điều khiển truy nhập bắt buộc) là gì?

a) DAC sử dụng vai trò, MAC sử dụng luật.

b) Trong DAC, chủ sở hữu quyết định quyền truy nhập; trong MAC, hệ thống/quản trị viên quyết định dựa trên chính sách và nhãn bảo mật.

c) DAC chỉ áp dụng cho file, MAC áp dụng cho hệ thống.

d) DAC kém an toàn hơn MAC trong mọi trường hợp.

10. Ma trận điều khiển truy nhập (ACM) mô tả mối quan hệ giữa các thành phần nào?

a) Người dùng, Vai trò, Quyền.

b) Chủ thể, Luật, Hành động.

c) Chủ thể (Subject), Đối tượng (Object), Quyền truy nhập (Access Right).

d) Nhóm người dùng, Chính sách, Tài nguyên.

11. Nguyên tắc "đọc xuống" (read-down) trong mô hình Bell-LaPadula có nghĩa là gì?

a) Người dùng chỉ được đọc các đối tượng ở mức bảo mật cao hơn mình.

b) Người dùng ở mức bảo mật k chỉ có thể đọc các đối tượng ở cùng mức hoặc thấp hơn.

c) Người dùng không được phép đọc bất kỳ đối tượng nào.

d) Người dùng có thể đọc mọi đối tượng bất kể mức bảo mật.

12. Điều khiển truy nhập dựa trên vai trò (RBAC) mang lại lợi ích chính nào so với việc gán quyền trực tiếp cho từng người dùng?

a) Tăng cường tính bí mật tuyệt đối cho dữ liệu.

b) Loại bỏ hoàn toàn nhu cầu xác thực người dùng.

c) Đơn giản hóa việc quản lý quyền khi có nhiều người dùng và tài nguyên, dễ dàng thay đổi quyền theo chức vụ.

d) Cho phép người dùng tự do chia sẻ tài nguyên không giới hạn.

13. Firewalls thường áp dụng loại biện pháp điều khiển truy nhập nào?

a) Điều khiển truy nhập tuỳ chọn (DAC).

b) Điều khiển truy nhập bắt buộc (MAC).

c) Điều khiển truy nhập dựa trên vai trò (RBAC).

d) Điều khiển truy nhập dựa trên luật (Rule-Based AC).

14. Tại sao mật khẩu mạnh nên bao gồm nhiều loại ký tự (thường, hoa, số, đặc biệt) và có độ dài đủ lớn?

a) Để dễ nhớ hơn cho người dùng.

b) Để tăng độ phức tạp, khiến việc đoán hoặc tấn công brute-force trở nên khó khăn hơn đáng kể.

c) Để tương thích với nhiều hệ thống khác nhau.

d) Để hệ thống có thể mã hóa mật khẩu nhanh hơn.

15. Chứng chỉ số (Digital Certificate) thường chứa thông tin gì quan trọng để xác thực?

a) Chỉ chứa mật khẩu của chủ thể.

b) Chỉ chứa khóa bí mật của chủ thể.

c) Thông tin nhận dạng chủ thể, khóa công khai của chủ thể, và chữ ký số của tổ chức phát hành (CA).

d) Lịch sử truy cập của chủ thể.

16. Ưu điểm chính của việc sử dụng đặc điểm sinh trắc học để điều khiển truy nhập là gì?

a) Chi phí triển khai thấp và tốc độ nhận dạng nhanh.

b) Không bao giờ xảy ra lỗi nhận dạng sai.

c) Đặc điểm sinh trắc học là duy nhất và luôn đi cùng chủ thể, khó bị đánh cắp hoặc quên như mật khẩu/thẻ.

d) Dễ dàng chia sẻ quyền truy cập cho người khác.

17. Trong mô hình Bell-LaPadula, nguyên tắc "ghi lên" (write-up) nhằm mục đích gì?

a) Cho phép người dùng ghi dữ liệu vào bất kỳ đối tượng nào có mức bảo mật thấp hơn.

b) Đảm bảo người dùng có thể sửa đổi mọi thông tin họ đọc được.

c) Ngăn chặn việc rò rỉ thông tin từ mức bảo mật cao xuống mức thấp hơn thông qua hành động ghi.

d) Cho phép người dùng ở mức bảo mật cao ghi đè dữ liệu ở mức thấp.

18. So sánh giữa Thẻ thông minh (Smartcard) và Thẻ bài (Token) dựa trên nội dung bài giảng, điểm khác biệt chính về khả năng là gì?

a) Smartcard sử dụng xác thực 2 yếu tố, còn Token thì không.

b) Token chỉ lưu trữ mật khẩu tĩnh, Smartcard lưu trữ OTP.

c) Token thường có năng lực tính toán (CPU, bộ nhớ) cao hơn Smartcard, cho phép cơ chế xác thực mạnh hơn.

d) Smartcard luôn yêu cầu tiếp xúc vật lý, còn Token thì không.

19. Một hệ thống áp dụng MAC với các mức bảo mật: Unclassified (U), Confidential (C), Secret (S), Top Secret (T). Một người dùng có mức clearance là Secret (S). Theo mô hình Bell-LaPadula, người dùng này KHÔNG thể thực hiện hành động nào sau đây?

a) Đọc một tài liệu được đánh dấu Confidential (C).

b) Ghi vào một tài liệu được đánh dấu Secret (S).

c) Đọc một tài liệu được đánh dấu Top Secret (T).

d) Ghi vào một tài liệu được đánh dấu Top Secret (T).

20. Tại sao việc chỉ dựa vào một yếu tố xác thực (ví dụ: chỉ mật khẩu) lại tiềm ẩn nhiều rủi ro hơn so với xác thực đa yếu tố (ví dụ: thẻ + PIN, hoặc mật khẩu + OTP)?

a) Xác thực đa yếu tố luôn nhanh hơn xác thực đơn yếu tố.

b) Nếu yếu tố xác thực duy nhất bị lộ (ví dụ: mật khẩu bị đánh cắp), kẻ tấn công có thể truy cập hệ thống. Xác thực đa yếu tố yêu cầu kẻ tấn công phải có được nhiều hơn một yếu tố, tăng cường đáng kể độ an toàn.

c) Xác thực đơn yếu tố không thể áp dụng cho các hệ thống quan trọng.

d) Xác thực đa yếu tố rẻ hơn để triển khai.

Mục 4.2: Tường lửa (Firewall)

1. Tường lửa (Firewall) là gì?

a) Một phần mềm diệt virus.

b) Một hệ thống an ninh mạng kiểm soát lưu lượng mạng vào/ra dựa trên các quy tắc bảo mật.

c) Một thiết bị lưu trữ dữ liệu mạng.

d) Một công cụ mã hóa dữ liệu.

2. Chức năng chính của tường lửa là gì?

a) Tăng tốc độ kết nối mạng.

b) Sao lưu dữ liệu hệ thống.

c) Bảo vệ mạng nội bộ khỏi các truy cập trái phép từ bên ngoài và kiểm soát truy cập ra ngoài.

d) Quản lý tài khoản người dùng.

3. Vùng DMZ (Demilitarized Zone) trong kiến trúc mạng có tường lửa thường được sử dụng để đặt các máy chủ nào?

a) Máy chủ cơ sở dữ liệu nội bộ.

b) Máy chủ cung cấp dịch vụ công cộng (Web server, Mail server).

c) Máy trạm của người dùng nội bộ.

d) Máy chủ quản lý tên miền (DNS) nội bộ.

4. Loại tường lửa nào hoạt động ở tầng mạng (Network Layer) và kiểm tra thông tin header của gói tin?

a) Tường lửa lọc gói tin (Packet Filtering Firewall).

b) Tường lửa cổng ứng dụng (Application Gateway Firewall).

c) Tường lửa cổng chuyển mạch (Circuit-Level Gateway Firewall).

d) Tường lửa trạng thái (Stateful Firewall).

5. Tường lửa cổng ứng dụng (Application Gateway Firewall) hoạt động ở tầng nào trong mô hình OSI?

a) Tầng Vật lý (Physical Layer).

b) Tầng Liên kết dữ liệu (Data Link Layer).

c) Tầng Mạng (Network Layer).

d) Tầng Ứng dụng (Application Layer).

6. Kỹ thuật kiểm soát truy nhập nào KHÔNG phải là một trong các kỹ thuật được tường lửa sử dụng?

a) Service control (Kiểm soát dịch vụ).

b) Direction control (Kiểm soát hướng).

c) User control (Kiểm soát người dùng).

d) Content control (Kiểm soát nội dung - thường là chức năng của proxy/web filter).

7. Đâu là một hạn chế của tường lửa?

a) Không thể kiểm soát lưu lượng vào/ra.

b) Không thể bảo vệ chống lại các cuộc tấn công không đi qua tường lửa (ví dụ: tấn công nội bộ, virus qua USB).

c) Không thể lọc gói tin dựa trên địa chỉ IP.

d) Không thể hoạt động ở tầng ứng dụng.

8. Tường lửa "lọc gói tin" (Packet Filtering) đưa ra quyết định dựa trên thông tin nào?

a) Nội dung đầy đủ của gói tin.

b) Trạng thái của kết nối.

c) Địa chỉ IP nguồn/đích, cổng nguồn/đích, giao thức.

d) Thông tin người dùng đang gửi gói tin.

9. Sự khác biệt chính giữa tường lửa lọc gói tin (Packet Filtering) và tường lửa cổng ứng dụng (Application Gateway) là gì?

a) Lọc gói tin nhanh hơn nhưng kém an toàn hơn.

b) Lọc gói tin hoạt động ở tầng mạng, kiểm tra header; Cổng ứng dụng hoạt động ở tầng ứng dụng, hiểu giao thức và có thể kiểm tra nội dung.

c) Cổng ứng dụng không thể lọc dựa trên địa chỉ IP.

d) Lọc gói tin chỉ dùng cho mạng nhỏ, cổng ứng dụng dùng cho mạng lớn.

10. Tường lửa cổng chuyển mạch (Circuit-Level Gateway) hoạt động như thế nào?

a) Kiểm tra chi tiết nội dung của từng gói tin ứng dụng.

b) Thiết lập kết nối TCP giữa client và proxy, sau đó proxy thiết lập kết nối thay mặt client đến server đích, không kiểm tra nội dung ứng dụng.

c) Chỉ lọc dựa trên địa chỉ IP và cổng.

d) Hoạt động dựa trên vai trò của người dùng.

11. Tường lửa trạng thái (Stateful Inspection Firewall) khác biệt với tường lửa lọc gói tin không trạng thái (Stateless Packet Filtering) ở điểm nào?

a) Tường lửa trạng thái chậm hơn đáng kể.

b) Tường lửa trạng thái theo dõi trạng thái các kết nối đang hoạt động và đưa ra quyết định lọc dựa trên ngữ cảnh của kết nối, không chỉ dựa trên từng gói tin riêng lẻ.

c) Tường lửa không trạng thái an toàn hơn.

d) Tường lửa trạng thái chỉ hoạt động ở tầng ứng dụng.

12. Tại sao việc đặt tường lửa giữa mạng nội bộ và Internet lại quan trọng?

a) Để tăng băng thông Internet.

b) Để lưu trữ cache các trang web thường truy cập.

c) Để tạo ra một điểm kiểm soát duy nhất, ngăn chặn truy cập trái phép từ Internet vào mạng nội bộ và kiểm soát truy cập ra ngoài.

d) Để mã hóa toàn bộ lưu lượng mạng.

13. Mô hình tôpô mạng nào sử dụng hai tường lửa để tạo ra một vùng DMZ an toàn hơn?

a) Single firewall with one interface.

b) Single firewall with two interfaces.

c) Dual firewall configuration (Screened subnet firewall).

d) Host-based firewall configuration.

14. Kỹ thuật "Service control" trong tường lửa cho phép làm gì?

a) Xác định các loại dịch vụ Internet có thể được truy cập, vào trong hay ra ngoài.

b) Xác định người dùng nào được phép truy cập dịch vụ.

c) Xác định hướng của luồng dữ liệu được phép.

d) Xác định thời gian truy cập dịch vụ.

15. Tường lửa lọc gói tin (Packet Filtering) có thể gặp khó khăn trong việc chống lại loại tấn công nào?

a) Tấn công từ chối dịch vụ (DoS) dựa trên số lượng lớn gói tin.

b) Tấn công khai thác lỗ hổng ở tầng ứng dụng (vì nó không kiểm tra nội dung ứng dụng).

c) Chặn truy cập từ một địa chỉ IP cụ thể.

d) Chặn truy cập đến một cổng dịch vụ cụ thể.

16. Hạn chế nào của tường lửa liên quan đến việc không thể bảo vệ chống lại các mối đe dọa từ bên trong mạng?

a) Tường lửa không thể lọc lưu lượng mã hóa.

b) Tường lửa làm chậm tốc độ mạng.

c) Tường lửa thường được đặt ở biên mạng và không giám sát/kiểm soát lưu lượng hoàn toàn bên trong mạng nội bộ.

d) Tường lửa không thể cập nhật các quy tắc mới.

17. So sánh giữa tường lửa lọc gói tin trạng thái (Stateful) và tường lửa cổng ứng dụng (Application Gateway), lựa chọn nào thường cung cấp mức độ bảo mật cao nhất nhưng có thể ảnh hưởng đến hiệu năng nhiều nhất?

a) Tường lửa lọc gói tin không trạng thái (Stateless).

b) Tường lửa lọc gói tin trạng thái (Stateful).

c) Tường lửa cổng ứng dụng (Application Gateway / Proxy Firewall).

d) Tường lửa cổng chuyển mạch (Circuit-Level Gateway).

18. Tại sao tường lửa trạng thái (Stateful Firewall) lại an toàn hơn tường lửa lọc gói tin không trạng thái (Stateless)?

a) Vì nó kiểm tra nội dung dữ liệu ứng dụng.

b) Vì nó hiểu ngữ cảnh của luồng giao tiếp, chỉ cho phép các gói tin phản hồi hợp lệ tương ứng với các yêu cầu đã được khởi tạo từ bên trong đi qua, chống lại các kỹ thuật quét và giả mạo gói tin tinh vi hơn.

c) Vì nó hoạt động ở tầng ứng dụng.

d) Vì nó có thể xác thực người dùng.

19. Trong một cấu hình tường lửa kép (dual firewall) cho DMZ, tường lửa bên ngoài (external firewall) và tường lửa bên trong (internal firewall) thường có các bộ quy tắc khác nhau như thế nào?

a) Cả hai có bộ quy tắc giống hệt nhau.

b) Tường lửa bên ngoài cho phép mọi thứ, tường lửa bên trong chặn mọi thứ.

c) Tường lửa bên ngoài cho phép truy cập hạn chế từ Internet vào DMZ; Tường lửa bên trong cho phép truy cập hạn chế từ DMZ vào mạng nội bộ và kiểm soát chặt chẽ hơn truy cập từ mạng nội bộ ra DMZ/Internet.

d) Tường lửa bên trong cho phép mọi thứ, tường lửa bên ngoài chặn mọi thứ.

20. Tường lửa thế hệ tiếp theo (Next-Generation Firewall - NGFW) thường tích hợp thêm những khả năng nào so với tường lửa trạng thái truyền thống?

a) Chỉ lọc gói tin dựa trên IP và cổng.

b) Chỉ hoạt động như một cổng chuyển mạch.

c) Nhận dạng ứng dụng (Application awareness), hệ thống ngăn chặn xâm nhập (IPS), kiểm soát người dùng dựa trên danh tính, và đôi khi là lọc nội dung web.

d) Chỉ cung cấp kết nối VPN.

Mục 4.3: Các hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS)

1. IDS là viết tắt của thuật ngữ nào?

a) Intrusion Detection Standard

b) Intrusion Detection System

c) Internet Defense System

d) Intrusion Defense Standard

2. Chức năng chính của Hệ thống phát hiện xâm nhập (IDS) là gì?

a) Ngăn chặn mọi cuộc tấn công mạng.

b) Giám sát lưu lượng mạng hoặc hoạt động hệ thống để phát hiện các hoạt động đáng ngờ hoặc độc hại và đưa ra cảnh báo.

c) Mã hóa dữ liệu truyền trên mạng.

d) Quản lý tường lửa.

3. IPS là viết tắt của thuật ngữ nào?

a) Intrusion Prevention Standard

b) Internet Protection System

c) Intrusion Prevention System

d) Intrusion Protection Standard

4. Sự khác biệt cơ bản giữa IDS và IPS là gì?

a) IDS giám sát mạng, IPS giám sát máy chủ.

b) IDS chỉ phát hiện tấn công dựa trên chữ ký, IPS chỉ dựa trên bất thường.

c) IDS chỉ phát hiện và cảnh báo, còn IPS có khả năng phát hiện và chủ động ngăn chặn cuộc tấn công.

d) IDS đắt tiền hơn IPS.

5. NIDS (Network-based IDS) được đặt ở đâu trong mạng?

a) Trên từng máy chủ riêng lẻ.

b) Tại các điểm chiến lược trong mạng để giám sát lưu lượng của toàn bộ phân đoạn mạng.

c) Bên ngoài tường lửa.

d) Tích hợp vào trình duyệt web.

6. HIDS (Host-based IDS) giám sát hoạt động ở đâu?

a) Toàn bộ lưu lượng mạng.

b) Trên một máy chủ hoặc thiết bị đầu cuối cụ thể (ví dụ: file hệ thống, log hệ thống, tiến trình).

c) Lưu lượng giữa các mạng khác nhau.

d) Hoạt động của tường lửa.

7. Phương pháp phát hiện xâm nhập dựa trên chữ ký (Signature-based detection) hoạt động như thế nào?

a) Phân tích hành vi bất thường của người dùng.

b) So sánh lưu lượng mạng hoặc hoạt động hệ thống với một cơ sở dữ liệu các mẫu tấn công đã biết (chữ ký).

c) Dự đoán các cuộc tấn công trong tương lai.

d) Xây dựng mô hình hoạt động bình thường của hệ thống.

8. Đâu là một ví dụ về phần mềm NIDS mã nguồn mở phổ biến?

a) OSSEC

b) Windows Defender

c) Snort

d) Wireshark

9. Ưu điểm chính của phương pháp phát hiện dựa trên chữ ký (Signature-based) là gì?

a) Có thể phát hiện các cuộc tấn công chưa từng biết (zero-day).

b) Độ chính xác cao và tỷ lệ báo động giả (false positive) thấp đối với các tấn công đã biết.

c) Không cần cập nhật cơ sở dữ liệu chữ ký.

d) Phát hiện tốt các biến thể nhỏ của tấn công.

10. Nhược điểm chính của phương pháp phát hiện dựa trên chữ ký (Signature-based) là gì?

a) Tỷ lệ báo động giả rất cao.

b) Khó triển khai và quản lý.

c) Không thể phát hiện các cuộc tấn công mới hoặc các biến thể chưa có trong cơ sở dữ liệu chữ ký.

d) Yêu cầu tài nguyên hệ thống rất lớn.

11. Phương pháp phát hiện xâm nhập dựa trên bất thường (Anomaly-based detection) hoạt động như thế nào?

a) So sánh lưu lượng với các mẫu tấn công đã biết.

b) Xây dựng một mô hình (baseline) về hành vi bình thường của mạng hoặc hệ thống và cảnh báo khi phát hiện các hoạt động lệch khỏi mô hình đó.

c) Chỉ giám sát các file hệ thống.

d) Dựa vào danh sách đen các địa chỉ IP.

12. Ưu điểm chính của phương pháp phát hiện dựa trên bất thường (Anomaly-based) là gì?

a) Không bao giờ tạo ra báo động giả.

b) Không cần xây dựng mô hình hoạt động bình thường.

c) Có khả năng phát hiện các cuộc tấn công mới hoặc chưa biết (zero-day) mà phương pháp dựa trên chữ ký bỏ lỡ.

d) Rất dễ cấu hình và không cần đào tạo.

13. Nhược điểm chính của phương pháp phát hiện dựa trên bất thường (Anomaly-based) là gì?

a) Không thể phát hiện tấn công đã biết.

b) Có thể có tỷ lệ báo động giả (false positive) cao do khó xác định chính xác hành vi bình thường và các thay đổi hợp lệ có thể bị coi là bất thường.

c) Yêu cầu cập nhật chữ ký liên tục.

d) Chỉ hoạt động hiệu quả trên các máy chủ riêng lẻ.

14. Tại sao việc kết hợp cả NIDS và HIDS lại mang lại hiệu quả bảo mật tốt hơn?

a) Giảm chi phí triển khai.

b) Cung cấp cái nhìn đa lớp: NIDS giám sát lưu lượng mạng tổng thể, HIDS cung cấp chi tiết về hoạt động trên từng máy chủ cụ thể, bổ sung cho nhau.

c) Loại bỏ hoàn toàn báo động giả.

d) Chỉ cần cập nhật một cơ sở dữ liệu duy nhất.

15. Một IPS khi phát hiện tấn công có thể thực hiện hành động ngăn chặn nào?

a) Chỉ gửi cảnh báo cho quản trị viên.

b) Ghi lại log sự kiện.

c) Chặn lưu lượng từ địa chỉ IP nguồn, kết thúc phiên kết nối, hoặc sửa đổi gói tin độc hại.

d) Yêu cầu người dùng xác thực lại.

16. "False Positive" trong ngữ cảnh IDS/IPS có nghĩa là gì?

a) Hệ thống không phát hiện được một cuộc tấn công thực sự (bỏ lọt).

b) Hệ thống cảnh báo một hoạt động là tấn công trong khi thực tế đó là hoạt động bình thường/hợp lệ.

c) Hệ thống phát hiện chính xác một cuộc tấn công.

d) Hệ thống bị kẻ tấn công vô hiệu hóa.

17. Kỹ thuật "Stateful Protocol Analysis" trong phát hiện bất thường hoạt động dựa trên nguyên tắc nào?

a) So sánh các gói tin với chữ ký tấn công đã biết.

b) Phân tích tần suất xuất hiện của các loại gói tin.

c) Hiểu rõ các trạng thái và trình tự hợp lệ của một giao thức mạng cụ thể (ví dụ: HTTP, DNS) và phát hiện các sai lệch hoặc hành vi vi phạm giao thức đó.

d) Xây dựng hồ sơ hành vi của từng người dùng.

18. Tại sao việc cập nhật thường xuyên cơ sở dữ liệu chữ ký lại quan trọng đối với IDS/IPS dựa trên chữ ký?

a) Để giảm tỷ lệ báo động giả.

b) Để tăng tốc độ xử lý của hệ thống.

c) Để đảm bảo hệ thống có thể nhận diện được các mối đe dọa và các biến thể tấn công mới nhất vừa được phát hiện và định nghĩa.

d) Để hệ thống có thể phát hiện tấn công zero-day.

19. Một thách thức khi triển khai IDS/IPS dựa trên bất thường trong môi trường mạng động (thường xuyên thay đổi cấu hình, ứng dụng) là gì?

a) Khó tìm được chữ ký phù hợp.

b) Mô hình hành vi bình thường (baseline) trở nên khó xây dựng và duy trì chính xác, dẫn đến tăng nguy cơ báo động giả (false positive) hoặc bỏ lọt (false negative).

c) Yêu cầu băng thông mạng rất lớn.

d) Không tương thích với các thiết bị mạng hiện đại.

20. So sánh giữa NIDS và HIDS, loại nào có khả năng phát hiện tấn công trên lưu lượng mạng đã được mã hóa (ví dụ: HTTPS) tốt hơn và tại sao?

a) NIDS, vì nó thấy toàn bộ lưu lượng.

b) NIDS, vì nó có thể giải mã mọi loại mã hóa.

c) HIDS, vì nó hoạt động trên máy chủ nơi dữ liệu đã được giải mã trước khi xử lý bởi ứng dụng, trong khi NIDS thường chỉ thấy lưu lượng mã hóa trên đường truyền.

d) Cả hai đều không thể phát hiện tấn công trên lưu lượng mã hóa.