**1. Discuss the questions**1. What does the word *method* mean? - Từ method nghĩa là gì

Method dịch ra là phương pháp, phương thức đặc biệt để gải quyết một việc gì đó. Trong lập trình hướng đối tượng, phương thức đại diện cho các hành vi, hoạt động. Ví dụ với đối tượng là con người có các hành vi là đi, chạy, nhảy, ..  
2. What IDPS method do you know? - Bạn biết gì về phương thức IDPS

3. How many IDPS methods do you know? What are they?

Có 3 loại phương thức IDPS: Signature-Based IDPS (IDPS dựa trên chữ ký số), Statistical Anomaly-Based IDPS (IDPS dựa trên thống kê bất thường), Stateful Protocol Analysis IDPS (IDPS phân tích giao thức trạng thái  
4. What do the terms: *Signature-Based IDPS, Statistical Anomaly-Based IDPS,* and *Stateful Protocol Analysis IDPS* mean in your language?

**2. Read the text and do the tasks below**

**IDPS Detection Methods**

IDPSs use a variety of detection methods to monitor and evaluate network traffic. Three methods dominate: the signature-based approach, the statistical-anomaly approach, and the stateful packet inspection approach.

IDPS sử dụng nhiều phương pháp phát hiện khác nhau để theo dõi và đánh giá lưu lượng mạng. Ba phương pháp chiếm ưu thế: cách tiếp cận dựa trên chữ ký số, cách tiếp cận bất thường thống kê và phương pháp kiểm tra gói trạng thái.

**Signature-Based IDPS**

A signature-based IDPS (sometimes called a knowledge-based IDPS or a misuse detection IDPS) examines network traffic in search of patterns that match known signatures—that is, preconfigured , predetermined attack patterns.

Signature-based IDPS technology is widely used because many attacks have clear and distinct signatures, for example: (1) footprinting and fingerprinting activities use ICMP, DNS querying, and e-mail routing analysis; (2) exploits use a specific attack sequence designed to take advantage of a vulnerability to gain access to a system; (3) DoS and DDoS attacks, during which the attacker tries to prevent the normal usage of a system, overload the system with requests so that the system’s ability to process them efficiently is compromised or disrupted.

A potential problem with the signature-based approach is that new attack strategies must continually be added into the IDPS’s database of signatures; otherwise, attacks that use new strategies will not be recognized and might succeed. Another weakness of the signature based method is that a slow, methodical attack might escape detection if the relevant IDPS attack signature has a shorter time frame.

The only way a signature-based IDPS can resolve this vulnerability is to collect and analyze data over longer periods of time, a process that requires substantially larger data storage capability and additional processing capacity.

(Hệ thống phát hiện và ngăn chặn xâm nhập dựa trên chữ ký số : HTPHVNC (Viết tắt))

Hệ thống phát hiện và ngăn chặn xâm nhập dựa trên chữ ký số (đôi khi được gọi là HTPHVNC dựa trên kiến thức hoặc HTPHVNC phát hiện lạm dụng) kiểm tra lưu lượng mạng để tìm kiếm các mẫu phù hợp với chữ ký số đã biết - nghĩa là các kiểu tấn công được cấu hình trước, được xác định trước.

Công nghệ HTPHVNC dựa trên chữ ký số được sử dụng rộng rãi vì nhiều cuộc tấn công có chữ ký số rõ ràng và khác biệt, ví dụ: (1) dấu chân và dấu vân tay sử dụng phân tích định tuyến HTPHVNC, truy vấn DNS và e-mail; (2) khai thác sử dụng một chuỗi tấn công cụ thể được thiết kế để tận dụng lỗ hổng, truy cập vào hệ thống; (3) Các cuộc tấn công DoS và DDoS, trong đó kẻ tấn công cố gắng làm gián đoạn một hệ thống, làm hệ thống quá tải với các yêu cầu để khả năng xử lý của hệ thống không hiệu quả, bị xâm nhập hoặc bị gián đoạn.

Một nguy cơ tiềm ẩn với phương pháp dựa trên chữ ký số là các kiểu tấn công mới phải liên tục được thêm vào cơ sở dữ liệu chữ ký số của HTPHVNC; nếu không, các cuộc tấn công sử dụng các kiểu mới sẽ không bị phát hiện và có thể thực hiện thành công. Một điểm yếu khác của phương pháp dựa trên chữ ký số là nó không được nhanh, các cuộc tấn công có phương pháp có thể thoát khỏi sự phát hiện nếu cuộc tấn công chữ ký số của HTPHVNC có liên quan có khung thời gian ngắn hơn.

Cách duy nhất một HTPHVNC dựa trên chữ ký số có thể giải quyết lỗ hổng này là thu thập và phân tích dữ liệu trong thời gian dài hơn, một quá trình đòi hỏi khả năng lưu trữ dữ liệu lớn hơn đáng kể và khả năng xử lý bổ sung.

**Statistical Anomaly-Based IDPS**

The statistical anomaly-based IDPS (stat IDPS) or behavior-based IDPS collects statistical summaries by observing traffic that is known to be normal. This normal period of evaluation establishes a performance baseline. Once the baseline is established, the stat IDPS periodically samples network activity and, using statistical methods, compares the sampled network activity to this baseline. When the measured activity is outside the baseline parameters—exceeding what is called the clipping level—the IDPS sends an alert to the administrator. The baseline data can include variables such as host memory or CPU usage, network packet types, and packet quantities.

The advantage of the statistical anomaly-based approach is that the IDPS can detect new types of attacks, since it looks for abnormal activity of any type. Unfortunately, these systems require much more overhead and processing capacity than signature-based IDPSs, because they must constantly compare patterns of activity against the baseline. Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives. If the actions of the users or systems on a network vary widely, with periods of low activity interspersed with periods of heavy packet traffic, this type of IDPS may not be suitable, because the dramatic swings from one level to another will almost certainly generate false alarms. Because of its complexity and impact on the overhead computing load of the host computer as well as the number of false positives it can generate, this type of IDPS is less commonly used than the signature-based type.

HTPHVNC dựa trên thống kê bất thường hoặc HTPHVNC dựa trên hành vi thu thập các bản tóm tắt thống kê bằng cách quan sát lưu lượng thông thường. Khoảng thời gian đánh giá thông thường này thiết lập một đường cơ sở hiệu suất. Sau khi đường cơ sở được thiết lập, các chỉ số định kỳ của HTPHVNC lấy mẫu hoạt động mạng, bằng cách sử dụng các phương pháp thống kê, so sánh mẫu hoạt động mạng lấy được với đường cơ sở này. Khi đo được các thông số nằm ngoài các thông số cơ bản — vượt quá mức được gọi là mức cắt — HTPHVNC sẽ gửi một cảnh báo đến quản trị viên. Dữ liệu cơ sở có thể bao gồm các biến như bộ nhớ máy chủ hoặc mức sử dụng CPU, loại gói mạng và số lượng các gói.

Ưu điểm của cách tiếp cận dựa trên sự bất thường thống kê là HTPHVNC có thể phát hiện các kiểu tấn công mới, vì nó tìm kiếm hoạt động bất thường của bất kỳ kiểu tấn công nào. Thật không may, các hệ thống này yêu cầu chi phí và khả năng xử lý cao hơn nhiều so với HTPHVNC dựa trên chữ ký, bởi vì chúng phải liên tục so sánh các mô hình hoạt động với đường cơ sở. Một nhược điểm khác là các hệ thống này có thể không phát hiện ra những thay đổi nhỏ đối với các biến hệ thống và có thể tạo ra nhiều xác thực sai. Nếu hành động của người dùng hoặc hệ thống trên mạng rất rộng, với thời gian hoạt động thấp xen kẽ với thời gian lưu lượng gói lớn, loại hình HTPHVNC này có thể không phù hợp, bởi vì sự thay đổi đột ngột từ cấp độ này sang cấp độ khác gần như chắc chắn sẽ gây ra báo động sai. Do tính phức tạp và tác động lên tải tính toán chung của máy tính chủ cũng như số lần xác thực sai mà nó có thể tạo ra, loại HTPHVNC này ít được sử dụng hơn loại dựa trên chữ ký.

**Stateful Protocol Analysis IDPS**

According to SP 800-94, Stateful protocol analysis (SPA) is a process of comparing predetermined profiles of generally accepted definitions of benign activity for each protocol state against observed events to identify deviations.

Stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. Essentially, the IDPS knows how a protocol, such as FTP, is supposed to work, and therefore can detect anomalous behavior. By storing relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses, the IDPS can better detect specialized, multisession attacks. This process is sometimes called deep packet inspection because SPA closely examines packets at the application layer for information that indicates a possible intrusion. Stateful protocol analysis can also examine authentication sessions for suspicious activity as well as for attacks that incorporate “unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent, as well as ‘reasonableness’ for commands such as minimum and maximum lengths for arguments.” The models used for SPA are similar to signatures in that they are provided by vendors. These models are based on industry protocol standards established by such entities as the Internet Engineering Task Force, but they vary along with the protocol implementations in such documents. Also, proprietary protocols are not published in sufficient detail to enable the IDPS to comprehensive assessments.

Unfortunately, the analytical complexity of session-based assessments is the principal drawback to this type of IDPS method, which also requires heavy processing overhead to track multiple simultaneous connections. Additionally, unless a protocol violates its fundamental behavior, this IDPS method may completely fail to detect an intrusion. One final issue is that the IDPS may in fact interfere with the normal operations of the protocol it’s examining, especially with client- and server-differentiated operations.

Theo Tài liệu Hướng dẫn về Hệ thống phát hiện và ngăn chặn xâm nhập (SP 800-94) do Viện Tiêu chuẩn và Kỹ thuật quốc gia Hoa Kỳ (NIST) ban hành, phân tích giao thức trạng thái (SPA) là một quá trình so sánh các hồ sơ định trước của hoạt động của mỗi giao thức được coi là bình thường với đối tượng quan sát từ đó xác định độ lệch.

Phân tích giao thức trạng thái dựa trên các hồ sơ tổng quát do nhà cung cấp phát triển theo đó quy định 1 protocol nên làm và không nên làm gì.

Bản chất, HTPHVN biết như nào là một giao thức, chẳng hạn như FTP, được cho là phải hoạt động và do đó có thể phát hiện hành vi bất thường. Bằng cách lưu trữ dữ liệu có liên quan được phát hiện trong một phiên và sau đó sử dụng dữ liệu đó để xác định các hành vi xâm nhập liên quan đến nhiều yêu cầu và phản hồi, HTPHVN có thể phát hiện tốt hơn các cuộc tấn công chuyên biệt, đa nhiệm. Quá trình này đôi khi được gọi là kiểm tra gói tin sâu vì SPA kiểm tra chặt chẽ các gói tại lớp ứng dụng để biết thông tin nếu có sự xâm nhập. Phân tích giao thức trạng thái cũng có thể kiểm tra các phiên xác thực cho hoạt động đáng ngờ cũng như các cuộc tấn công kết hợp "chuỗi lệnh không mong muốn, chẳng hạn như phát hành cùng một lệnh lặp đi lặp lại hoặc phát hành lệnh mà không đưa ra lệnh trước mà nó phụ thuộc, cũng như ' tính hợp lý 'cho các lệnh chẳng hạn như độ dài tối thiểu và tối đa cho các đối số." Các mô hình được sử dụng cho SPA tương tự như chữ ký số ở chỗ chúng được cung cấp bởi các nhà cung cấp. Các mô hình này dựa trên các tiêu chuẩn giao thức công nghiệp được thiết lập bởi các đơn vị như Lực lượng Đặc nhiệm Kỹ thuật Internet, nhưng chúng thay đổi cùng với việc triển khai giao thức trong các tài liệu đó. Ngoài ra, các giao thức độc quyền không được công bố đầy đủ chi tiết để cho phép HTPHVN đánh giá toàn diện.

Thật không may, sự phức tạp phân tích của các đánh giá dựa trên phiên là nhược điểm chính của loại phương pháp HTPHVN, phương pháp này cũng đòi hỏi chi phí xử lý nặng để theo dõi nhiều kết nối đồng thời. Ngoài ra, trừ khi một giao thức vi phạm hành vi cơ bản của nó, nếu không thì phương pháp HTPHVN này không thể phát hiện ra sự xâm nhập. Một vấn đề cuối cùng là HTPHVN trên thực tế có thể can thiệp vào các hoạt động bình thường của giao thức mà nó đang kiểm tra, đặc biệt là với các hoạt động phân biệt giữa máy khách và máy chủ.