**Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập**

**Chương 1**

**Bộ ba CIA**

* Confidentiality (bảo mật): tránh để lộ thông tin trái phép
* Integrity (toàn vẹn): tránh để thông tin bị thay đổi trái phép
* Availability (sẵn sàng): đảm bảo những người dùng hợp lệ luôn có thể truy cập đến thông tin và hệ thống

**“intrusion”** - xâm nhập là một hành vi cố gắng xâm phạm CIA, hoặc qua mặt cơ chế bảo mật của một máy tính hoặc mạng máy tính.

“**intrusion detection**” – phát hiện xâm nhập là quy trình theo dõi các sự kiện diễn ra trong một hệ thống máy tính hoặc mạng máy tính và phân tích để nhận biết các dấu hiệu của sự bất thường.

“**Intrusion Detection System**” (IDS) – hệ thống phát hiện xâm nhập là hệ thống phần mềm hoặc phần cứng tự động thực hiện quy trình phát hiện xâm nhập.

“**Intrusion Prevention System**” (IPS) – hệ thống ngăn chặn xâm nhập là hệ thống có tất cả chức năng của IDS, và có thể dừng sự xâm nhập.

**Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập (IDPS)** chủ yếu tập trung vào xác định các sự cố có thể xảy ra, ghi nhận các thông tin liên quan, cố gắng ngăn chặn và báo cáo cho các quản trị viên bảo mật.

**Các IDS ngăn chặn xâm nhập**

IPS dừng hoạt động tấn công

1. Ngắt kết nối (mạng) hoặc phiên làm việc đang bị sử dụng để tấn công

* Chặn truy cập vào mục tiêu (hoặc các máy có khả năng là mục tiêu) từ tài khoản người dùng, địa chỉ IP hoặc các yếu tố tấn công khác.
* Chặn tất cả các truy cập đến host, dịch vụ, ứng dụng hoặc các tài nguyên khác là mục tiêu.

1. IPS thay đổi môi trường bảo mật

* Tái cấu hình một thiết bị mạng (ví dụ tường lửa, router, switch) để chặn truy cập từ attacker hoặc truy cập đến mục tiêu.
* Vá các lỗ hổng đang có trên host.

1. IPS thay đổi nội dung của hoạt động tấn công

* Loại bỏ hoặc thay thế những phần độc hại của tấn công để nó thành bình thường.
* Hoạt động như proxy và bình thường hoá các yêu cầu được gửi đến (đóng gói lại payloads của yêu cầu, bỏ các thông tin header…)

**Chương 2**

**Dựa trên Các kỹ thuật phát hiện tấn công**

* **Signature-based**

*Signature* là một mẫu tương ứng với một nguy cơ tấn công (cơ sở dữ liệu về các tấn công đã biết trước).

Kỹ thuật phát hiện *Signature-based* (hay còn gọi knowledge-based) là một quá trình so sánh các signature với các sự kiện quan sát được để xác định các sự cố có thể có.

Ưu điểm: Độ chính xác cao khi phát hiện các tấn công đã biết, tỉ lệ cảnh báo sai thấp.

Nhược điểm:

* Không thể phát hiện các hành vi bất thường chưa biết trước hoặc các biến đổi nhỏ trong những tấn công đã biết → Yêu cầu phải cập nhật liên tục cơ sở dữ liệu signature.
* Việc triển khai và cập nhật signature khó và tốn thời gian.
* **Anomaly-based**

Kỹ thuật phát hiện Anomaly-based (hoặc profile-based) hoạt động dựa trên việc:

* Tạo ra một profile cơ sở đại diện cho các hành vi bình thường/dự kiến trong mạng.
* Dựa trên đó, bất kỳ hoạt động mạng đang xem xét nào có sai khác so với profile này đều bị xem là bất thường.

*Profiles* đại diện cho hoạt động mạng bình thường hầu hết được tạo ra thông qua phân tích lịch sử lưu lượng mạng (qua các hàm thống kê, máy học, clustering, fuzzy logic, heuristics…)

Ưu điểm:

* Phát hiện được cả các hành vi bất thường đã biết và chưa biết, không cần phải có hiểu biết trước.
* Phát hiện được các tấn công mới (về sau có thể sử dụng trên các signature-based IDS).

Nhược điểm:

* Tỷ lệ false positives cao (phát hiện nhầm hành vi bình thường là tấn công).
* Ít hiệu quả quả trong các môi trường mạng động, thay đổi nhiều.
* Yêu cầu thời gian và tài nguyên để xây dựng được profile đại diện cho mạng.
* **Specification-based**

Kỹ thuật phát hiện Specification-based thu thập các hoạt động chính xác của một chương trình hoặc giao thức và theo dõi hoạt động của nó dựa trên các ràng buộc.

* Sử dụng mô hình giao thức chủ yếu dựa trên các chuẩn giao thức từ các nhà sản xuất phần mềm và tiêu chuẩn (IEFT, RFC).
* Ví dụ: Thực hiện nhiều câu lệnh (command) khi ở trạng thái chưa chứng thực trong FTP thường bị xem là bất thường.

Ưu điểm:

* Xác định được các chuỗi lệnh bất thường, kiểm tra được tính hợp lý của từng câu lệnh.
* Tỷ lệ false positive thấp.

Nhược điểm:

* Khó, thậm chí không thể phát triển các mô hình giao thức chính xác hoàn toàn.
* Phức tạp, tốn tài nguyên và thời gian
* **Hybrid (lai)**

Hybrid IDSs, hay còn gọi Compound Detection, kết hợp các kỹ thuật phát hiện dựa trên signature, anomaly và specification.

Ưu điểm:

* Đối phó được với các thay đổi tinh vi trong tấn công.
* Tích hợp được lợi ích của cả 3 kỹ thuật trước.
* Khắc phục được nhiều nhược điểm.

Nhược điểm:

* Bị giới hạn phạm vi vào hoạt động của một chương trình giao thức.
* Cần tích hợp sao cho 3 kỹ thuật riêng biệt có thể cùng tương tác và hoạt động trong cùng một hệ thống.

**Dựa trên Nguồn dữ liệu**

* **Network-based**

Network-based IDPS (NIDPS) theo dõi lưu lượng mạng cho một phần của mạng (network segment) hoặc các thiết bị, phân tích các hoạt động mạng và các giao thức, ứng dụng để xác định các hành vi bất thường.

* + Thường triển khai ở biên mạng, như gần tường lửa hoặc router biên, server VPN, server remote access và mạng không dây.
  + Gồm nhiều sensor đặt ở nhiều điểm khác nhau trong mạng để theo dõi lưu lượng mạng.
* **Host-based**

Host-based IDPS (HIDPS), theo dõi các đặc điểm của một host riêng lẻ và các sự kiện xảy ra trong host đó để phát hiện hoạt động bất thường. • Theo dõi: lưu lượng mạng của host, log hệ thống, các tiến trình đang chạy, các hoạt động ứng dụng, truy cập và thay đổi file, thay đổi trong cấu hình hệ thống hay ứng dụng,…

Được triển khai trên host quan trọng (các server có thể truy cập từ bên ngoài, các server chứa thông tin quan trọng).

* **Hybrid (lai)**

Hybrid IDPS được phát triển để hướng đến xem xét tất cả dữ liệu từ các sự kiện trên host và sự kiện trong các phần mạng, kết hợp chức năng của cả network và host-based IDPSs.

* + Tích hợp các ưu điểm của cả 2 kỹ thuật trên.
  + Cần tích hợp sao cho 2 kỹ thuật riêng biệt có thể cùng tương tác và hoạt động trong cùng một hệ thống.

**IDPS: Các thành phần chính**

* Sensor hoặc Agent: theo dõi và phân tích các hoạt động
  + Sensor: Network-based IDPS
  + Agent: Host-based IDPS
  + Server quản lý: thiết bị trung tâm quản lý.
  + Server cơ sở dữ liệu: nơi lưu trữ các thông tin tâm nhận các thông tin từ các sensor hoặc agent để theo dõi sự kiện.
  + Consoles: chương trình cung cấp giao diện tương tác với IDPS cho người dùng hoặc quản trị viên (GUI or CLI) .

Các thành phần của IDPS có thể được kết nối với nhau thông qua:

* Các mạng chuẩn (standard networks) của tổ chức, hoặc
* Một mạng tách biệt đc thiết kế riêng cho việc quản lý an toàn thông tin - **mạng quản lý**
* Ưu điểm:
  + Độc lập đối với mạng sản xuất của doanh nghiệp
  + Che giấu được sự tồn tại và dấu hiệu của IDPS với attacker
  + Bảo vệ IDPS khỏi tấn công và đảm bảo IDPS có đủ băng thông để hoạt động trong điều kiện bất lợi (do tấn công)
* Nhược điểm:
  + Cần thêm chi phí cho hạ tầng mạng và các phần cứng khác
  + Bất tiện cho người dùng và quản trị viên IDPS

**Kiến trúc Network-based IDPS**

* Các server quản lý, server cơ sở dữ liệu và console chỉ được gắn với mạng quản lý.
* Các sensor không thể gửi bất kỳ lưu lượng nào giữa interface quản lý của chúng với bất kỳ interface mạng nào khác của nó.

**IDPS: Các khả năng bảo mật**

1. Thu thập thông tin

Thu thập thông tin trên host hoặc mạng từ các hoạt động quan sát được.

1. Ghi log

* Ghi log các dữ liệu liên quan đến sự kiện phát hiện được
* Ghi log các dữ liệu có thể được dùng để kiểm tra **tính hợp lệ** của cảnh báo, điều tra các sự số và liên kết các sự kiện giữa IDPS và các nguồn log khác.
* Các trường dữ liệu phổ biến: thời gian xảy ra sự kiện, loại sự kiện, mức độ quan trọng (ví dụ độ ưu tiên, mức độ nghiêm trọng, tác động, độ tin cậy), hành động ngăn chặn đã thực hiện (nếu có), gói tin bắt được (NIDS), user ID (HIDS)
* Thông thường, log nên được lưu trữ ở cả nội bộ và tập trung để đảm bảo tính toàn vẹn và sẵn sàng của dữ liệu.

1. Phát hiện:

* Ngưỡng (thresholds): là 1 giá trị thiết lập giới hạn giữa hành vi bình thường và bất thường, xác định mức độ tối đa có thể chấp nhận được (là bình thường).
* Thường được dùng cho kỹ thuật phát hiện anomaly-based và phân tích các stateful protocol.
* Blacklists và Whitelist: là một danh sách các thực thể rời rạc đã được biết là bình thường, được sử dụng nhằm giảm hoặc loại bỏ các trường hợp false positive (dương tính giả) bao gồm các hoạt động bình thường từ các host đáng tin cậy.
  + thường sử dụng cho kỹ thuật phát hiện signature-based và phân tích các stateful protocol.
* Thiết lập cảnh báo
* Xem và chỉnh sửa mã nguồn

1. Ngăn chặn

* IDPS thường cho phép quản trị viên cấu hình khả năng ngăn chặn cho mỗi loại cảnh báo mà nó đưa ra.
* Thường bao gồm bật/tắt khả năng ngăn chặn, cũng như chỉ định rõ loại khả năng ngăn chặn nào nên dùng.

IDPS cần giao tiếp với các hệ thống nào khác?

* Hệ thống cung cấp dữ liệu (vd. DMZ server, log server tập trung, e-mail servers)
* Hệ thống để thực hiện các phản ứng ngăn chặn(vd., tường lửa, routers, switches)
* Hệ thống quản lý các thành phần IDPS (vd. phần mềm quản lý mạng hay bản vá)

**Chương 3**

**A screenshot of a computer

Description automatically generatedNetwork-based IDPS** thường chủ yếu phân tích tại tầng application, tầng transport và network, tuy nhiên, ít phân tích ở tầng network access.

Các thành phần chủ yếu: sensor, server quản lý, console, server cơ sở dữ liệu (optional)

Card mạng (Network interface card - NIC) được đặt ở **promiscuous mode** – mode dùng để theo dõi lưu lượng mạng. (Trong wifi gọi là Monitor Mode)

* Thông thường, card mạng (NIC) sẽ bỏ qua các gói tin không gửi đến nó (khác địa chỉ MAC).
* Khi hoạt động ở promiscuous mode, NIC chuyển tất cả các frame nhận được từ mạng đến kernel.
* Nếu một sniffer đã có đăng ký với kernel, nó có thể thấy tất cả các gói tin (frame) đó.

Sensor:

* Dựa trên thiết bị: gồm một phần cứng chuyên dụng (NICs hay driver NIC để bắt gói tin, bộ xử lý và các thành phần phần cứng khác cho việc phân tích), phần mềm sensor (firmware), và một hệ điều hành (OS) được tuỳ chỉnh.
* Chỉ gồm phần mềm: có thể bao gồm cả hệ điều hành (OS) được tuỳ chỉnh, hoặc có thể được cài đặt trên OS chuẩn của các host.

A diagram of a computer network

Description automatically generated

**Inline sensor**:

* Lưu lượng mạng được theo dõi đều phải đi qua sensor đó, tương tự như lưu lượng đi qua tường lửa.
* Cho phép ngăn chặn tấn công bằng cách chặn lưu lượng mạng.
* Một vài inline sensor là thiết bị lai firewall/IDPS (A) hoặc chỉ là IDPS (B)
* Đặt ở đâu?
  + A: Đặt tại vị trí của tường lửa mạng và các thiết bị bảo mật mạng khác (giữa các mạng, biên mạng)
  + B: Đặt ở một phía an toàn hơn của phần mạng để có ít traffic phải xử lý hơn.

**Passive sensor:**

* Theo dõi bản sao của lưu lượng mạng; không có lưu lượng thực tế nào đi qua sensor
* Vị trí?
  + Vị trí quan trọng trong mạng (như vị trí chia giữa các mạng)
  + Các segment mạng quan trọng (như vùng DMZ)

**Các phương pháp theo dõi mạng**

**Network TAPs** (Terminal Access Point):

* Kết nối trực tiếp giữa sensor và đường truyền vật lý
* Cung cấp bản sao các lưu lượng mạng trên đường truyền
* Fail-safe
* Nhược điểm: cần thêm chi phí trang bị

**Switch Port mirroring:** switch sao chép các frame của một hoặc nhiều port gửi đến SPAN (Switch Port Analyzer) port, có thể kết nối với thiết bị phân tích

* Nhược điểm: SPAN port có thể không thấy được tất cả lưu lượngnếu cấu hình sai hoặc đang quá tải.

**Công cụ theo dõi mạng**

* Bộ phân tích giao thức – Chương trình bắt lưu lượng mạng. Vd: Wireshark và Tcpdump
* NetFlow – Cung cấp đầy đủ các thông tin cơ bản về tất cả luồng IP chuyển tiếp trên 1 thiết bị
* SIEM – Security Information Event Management hỗ trợ báo cáo theo thời gian thực và phân tích các sự kiện bảo mật

*SNMP – Simple Network Management Protocol* cho phép yêu cầu và thu thập thông tin (thụ động) trên tất cả các thiết bị mạng

**Các khả năng bảo mật**

1. Thu thập thông tin

Thu thập cả thông tin trên các host và các hoạt động mạng chứa các host đó.

* Xác định các host dựa trên địa chỉ IP và MAC
* Xác định thông tin hệ điều hành OS
* Xác định các ứng dụng
* Xác định các đặc điểm của mạng

1. Ghi log
2. Phả hiện tấn công

Các dạng sự kiện có thể phát hiện:

* Do thám và tấn công ở tầng Application (banner grabbing, buffer overflows, format string, dò/đoán password, malware...)
* Do thám và tấn công ở tầng Transport (port scanning, packet fragmentation, SYN floods...)
* Do thám và tấn công ở tầng Network (giả mạo IP address, giá trị IP header không hợp lệ...)
* Các dịch vụ ứng dụng bất thường (backdoor, host chạy các dịch vụ ứng dụng trái phép...)
* Vi phạm chính sách (sử dụng website không phù hợp, sử dụng giao thức bị cấm...)

Các tổ chức nên sử dụng NIDPS để một phần nào đó có thể chống lại một số *kỹ thuật qua mặt (evasion technique)* phổ biến

**Hạn chế**

* Bị giới hạn hoặc không thể phân tích lưu lượng mạng đã mã hoá (kết nối VPN, (HTTPS), và session SSH).
* Xử lý tải lượng lưu lượng cao
  + Passive IDPS sensor có thể drop 1 vài gói, khiến phát hiện sai tấn công, đặc biệt khi phân tích stateful protocol
  + Inline IDPS sensor drop gói tin sẽ khiến mạng bị gián đoạn; hoặc chậm xử lýmgói tin dẫn đến độ trễ quá cao
* Hứng chịu các tấn công vào chính NIDPS
  + Attacker tạo lượng traffic lớn (vd: DDoS) hoặc các hoạt động bất thường (vd: gói tin bị fragment bất thường) để làm cạn kiệt tài nguyên của sensor và khiến sensor bị crash
  + Tạo lưu lượng mạng khiến NIDPS kích hoạt nhiều cảnh báo trong thời gian ngắn

**Ngăn chặn tấn công**

1. **Chỉ Passive mode**

Kết thúc phiên session TCP hiện tại bằng cách gửi gói TCP reset đến cả 2 đầu kết nối (session sniping)

* Chỉ thích hợp với TCP, không sử dụng được với các tấn công sử dụng UDP và ICMP
* Không còn được sử dụng rộng rãi

1. **Chỉ Inline mode**

Thực hiện chức năng tường lửa

Giới hạn băng thông: giới hạn tỉ lệ băng thông mạng mà giao thức có thể dùng

Thay đổi nội dung độc hại: thay thế nội dung độc hại bằng nội dung bình thường và gửi gói tin đã thay đổi đến host đích

1. **Cả Passive và Inline mode**

Tái cấu hình các thiết bị mạng khác. Chạy các chương trình hoặc script khác.

**Chương 4**

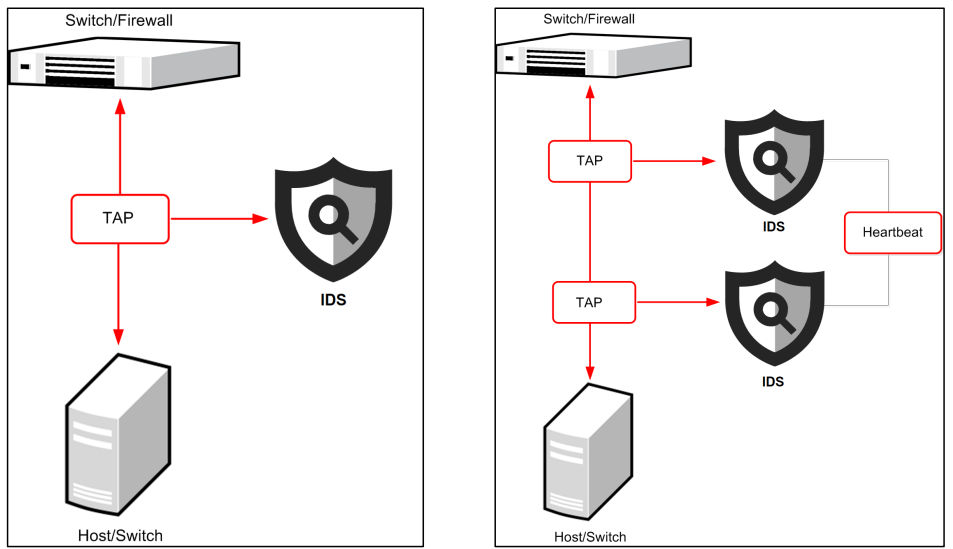
Triển khai IDS với Port mirroring

A diagram of a computer network

Description automatically generated

Triển khai IDS với network TAP

* Hai đầu Tap không có IP
* Xài 2 IDS để backup, một cái hư thì cái còn lại vẫn host bth



Triển khai IDS với Reset Interface

A diagram of a computer system

Description automatically generated

Triển khai IPS trong inline mode

A diagram of a cloud computing network

Description automatically generated

Inline mode bắt được ít traffic hơn port mirroring.

**Câu hỏi 1:** Snort thuộc loại NIDPS nào? Signature-based NIDPS

**Câu hỏi 2:** Snort có thể làm gì? (Có thể chọn nhiều đáp án)

A Bắt lưu lượng mạng đang truyền

B Phân tích các gói tin mạng thu thập được

C Ghi log các sự kiện, thông tin

D Nhận diện tấn công Chọn hết

**Câu hỏi 3:** Snort sử dụng … cho việc nhận diện tấn công.

A Một cơ sở dữ liệu tấn công đính kèm

B Một mô hình máy học phân loại lưu lượng bình thường hay tấn công

C Một tập các bộ rules định nghĩa dấu hiệu của tấn công

D Đáp án khác

**Câu hỏi 4:** Có thể truy cập vào các rules định nghĩa tấn công của Snort bằng cách nào?

A Snort cung cấp các tập rule mặc định kèm theo trong source cài đặt

B Người dùng có thể tự viết các rule của Snort

C Có nhiều tập rule dành cho các người dùng khác nhau trên trang chủ

D Cách nào cũng được

**Câu hỏi 5:** Snort có thể nhận lưu lượng mạng để phân tích từ nguồn nào?

A Lưu lượng mạng bắt được trên interface giám sát

B Từ 1 file pcap chứa lưu lượng mạng đã bắt trước đó

C Snort cân hết cả 2 nguồn trên ☺

D Chịu

**Câu hỏi 6:** Snort có cho phép chặn tấn công hay không?

A Mặc định là có

B Không

C Có nhưng chỉ ở chế độ phù hợp

D Chưa làm thử bao giờ

A screenshot of a computer

Description automatically generated

**Snort 2 rules**

* Định nghĩa các sự kiện/điều kiện mà Snort cần quan tâm, ví dụ như một tấn công, và hành động nên thực hiện khi sự kiện xảy ra.
* Rule options chia là nhiều nhóm option, quan trọng nhất là các **detection options** dùng để phát hiện tấn công.
* Các file .rules

A screenshot of a computer

Description automatically generated

**Chương 5**

2 thành phần trong mạng LAN cần được bảo vệ:

* **Endpoint** – Các hosts thường là các laptop, máy bàn, máy in, server, các điện thoại IP, …
* **Hạ tầng mạng** – Các thiết bị trong hạ tầng LAN kết nối các endpoint, thường bao gồm switch, thiết bị không dây, các thiết bị thoại IP...

**Endpoint Security**

**Làm sao để bảo vệ các endpoint?**

4 bước chính: **Discover → Inventory → Monitor → Protect**

Bộ giải pháp Host-based security – gồm antivirus, anti-phishing (chống lừa đảo), safe browsing, Host-based intrusion prevention system (HIDPS), firewall và chức năng ghi log.

Các phần mềm Antimalware/antivirus.

* Signature-based – Phát hiện các đặc điểm khác nhau của những file malware đã biết.
* Heuristics-based – Phát hiện các tính năng chung thường được sử dụng bởi các loại malware.
* Behavior-based – dựa trên việc phân tích các hành vi đáng ngờ.

**Host-based firewall** bao gồm:

* Windows Firewall – sử dụng hướng tiếp cận profile-based để cấu hình hoạt động của firewall.
* Iptables – cho phép cấu hình các rule kiểm soát truy cập trên các hệ thống Linux/
* Nftables – kế thừa từ iptables, nftables là ứng dụng firewall cho Linux sử dụng 1 máy ảo đơn giản trong kernel Linux.
* TCP Wrapper cho các thiết bị Linux – hệ thống kiểm soát truy cập và ghi log dựa trên rule.

Host-based IDPS theo dõi các đặc điểm của 1 host và các sự kiện xảy ra trong host đó (trong mạng LAN) để nhận biết các hành vi đáng ngờ.

* Theo dõi các traffic mạng có dây và không dây (chỉ cho host/server đó)
* Theo dõi log hệ thống, tiến trình đang chạy, các file, các hoạt động truy cập và thay đổi file, thay đổi trong cấu hình hệ thống và ứng dụng, registry (Windows)
* Đánh giá traffic do host đó tạo ra • Không lắng nghe các gói tin khi chúng đi vào mạng LAN

**Các thành phần:**

* Agent: phần mềm hoặc phần cứng chuyên dụng, thực hiện theo dõi các hoạt động trên 1 host, gửi dữ liệu đến các server quản lý
* Mỗi agent thường được thiết kế cụ thể để bảo vệ:
  + Một server: theo dõi hệ điều hành của server, một số ứng dụng phổ biến
  + Một client host (máy bàn hay laptop): theo dõi hệ điều hành và các ứng dụng client phổ biến như e-mail client, trình duyệt web, ...
  + Một dịch vụ ứng dụng: theo dõi một dịch vụ ứng dụng, như Web server hoặc server cơ sử dữ liệu (còn được gọi là application-based IDPS)
* Thường được triển khai trên các host quan trọng như các server có thể được truy cập từ internet và các server chứa thông tin quan trọng

**Kiến trúc mạng**

* Agent được triển khai trên các host đang có trong mạng của tổ chức, ***thay vì sử dụng một mạng quản lý riêng.***
* Hầu hết các sản phẩm HIDPS mã hoá giao tiếp để tránh việc bị nghe lén khi truy cập các thông tin quan trọng.
* Agent dựa trên phần cứng thường được triển khai inline ngay phía trước host cần được bảo vệ.

**Cần đặt các agent ở đâu?**

Có thể triển khai agent trên hầu hết các server và máy bàn/ laptop

Thường dùng để phân tích các hoạt động mà các biện pháp kiểm soát an ninh khác không theo dõi được

Ví dụ: network-based IDPS sensor không thể phân tích các hoạt động trong các kết nối mạng được mã hoá, nhưng host-based IDPS agent cài đặt trên các endpoint có thể theo dõi các hoạt động sau khi giải mã

Cần xem xét điều kiện gì khi lựa chọn vị trí cho các agent?

* Chi phí triển khai, vận hành và theo dõi các agent
* Các hệ điều hành và ứng dụng được agent hỗ trợ. Windows, MacOS, Android, IOS,...
* **A diagram of a computer

  Description automatically generated**Tầm quan trọng của dữ liệu hoặc dịch vụ trên các host
* Khả năng hỗ trợ các agent của hạ tầng

**Các kiến trúc Host**

Cấu hình HIDPS

* **Cấu hình tập trung**
  + Các agent gửi tất cả dữ liệu đến 1 vị trí trung tâm
  + Hiệu suất của host không bị ảnh hưởng bởi IDPS
  + A diagram of a process

    Description automatically generatedCác cảnh báo có thể k6hông theo thời gian thực

➔ Yêu cầu ít CPU, RAM, ổ cứng trên các host

* **Cấu hình phân tán**
  + Việc xử lý các sự kiện được phân tán giữa host và console
  + Host tạo và phân tích sự kiện theo thời gian thực
  + Giảm hiệu suất trên các host

➔ Các host nên được trang bị tối đa CPU, RAM, ổ cứng

**Hoạt động của HIDS**

HIDPS có khả năng ngăn chặn tấn công do sử dụng signature để phát hiện các xâm nhập đã biết và ngăn chúng ảnh hưởng đến hệ thống.

Có thể kết hợp chiến lược khác để phát hiện các xâm nhập qua mặt được kỹ thuật phát hiện signature-based (như Anomaly-based).

**Khả năng phát hiện tấn công**

Các loại sự kiện phát hiện được: chủ yếu dựa trên các kỹ thuật phát hiện sau:

* **Phân tích code**: xác định các hành động đáng ngờ nhờ phân tích các lần thực thi mã code.
  + Phân tích hoạt động của code: thực thi code trong sandbox để phân tích hành vi của nó
  + Phát hiện Buffer overflow: tìm các đặc điểm đặc trưng, như một chuỗi các instruction hay hành vi truy cập vào vùng nhớ khác vốn không được cấp phát cho tiến trình đó
  + Theo dõi lệnh gọi hệ thống (System call): biết ứng dụng hay tiến trình nào nên gọi ứng dụng hay tiến trình nào khác hoặc thực hiện các hành động nhất định. Agent có thể giới hạn driver nào có thể được load, để ngăn việc cài đặt rookit hoặc các tấn công khác
  + Danh sách ứng dụng và thư viện: để giới hạn các ứng dụng, thư viện cũng như phiên bản nhất định nào có thể được dùng
* **Phân tích lưu lượng mạng**: phân tích các ứng dụng thông dụng, client email phổ biến, trích xuất các file gửi bởi các ứng dụng như email, web và các file gửi peer-to-peer
* **Lọc lưu lượng mạng**: thường bao gồm 1 tường lửa host-based có thể giới hạn lưu lượng ra và vào cho mỗi ứng dụng trên hệ thống để ngăn chặn các truy cập trái phép và các hành vi vi phạm chính sách
* **Theo dõi hệ thống file (file system):** Kiểm tra tính toàn vẹn của file, kiểm tra các đặc điểm của file, theo dõi các truy cập file
* **Phân tích log**: theo dõi và phân tích các log của OS và ứng dụng để phát hiện hành vi bất thường.
* **Theo dõi cấu hình mạng**: theo dõi các cấu hình mạng hiện tại và phát hiện các thay đổi trên các cấu hình này
* **Độ chính xác**: Thách thức hơn với HIDPS ➔ Sử dụng kết hợp nhiều kỹ thuật phát hiện thường có thể đạt được khả năng phát hiện chính xác hơn so với sử dụng 1 hoặc một vài kỹ thuật
* Kết nối tự động HIDPS với các hệ thống quản lý thay đổi là không khả thi ➔ Quản trị viên có thể thường xuyên xem các record quản lý các thay đổi và thay đổi các cấu hình host và các policy trên HIDPS để ngăn false positive

**Các khả năng khác**

* **Giới hạn các thiết bị removable**: giới hạn sử dụng các thiết bị removable, cả dạng USB và truyền thống
* **Giám sát các thiết bị nghe nhìn**: giám sát các host khi kích hoạt hoặc sử dụng các thiết bị nghe nhìn, như microphone, camera, điện thoại IP,…
* **Host Hardening**: gỡ bỏ app không cần thiết; khóa port, dịch vụ không cần thiết; khóa/thay đổi tài khoản/mật khẩu mặc định,...
* **Theo dõi trạng thái tiến trình**: Một số sản phẩm theo dõi trạng thái các tiến trình/dịch vụ đang chạy trên host, nếu phát hiện đã dừng, các sản phẩm này có thể tự động khởi chạy lại chúng
* **Làm sạch (sanitize) lưu lượng mạng**: Một số agent, thường là loại triển khai dựa trên phần cứng, có thể làm sạch lưu mạng theo dõi được

**Các hạn chế**

* Độ trễ khi tạo cảnh báo và báo cáo tập trung:
  + Một số kỹ thuật được sử dụng để định kỳ xác định các sự kiện vốn đã diễn ra hoặc chỉ sử dụng theo giờ hoặc thậm chí chỉ vài lần trong ngày, tạo ra độ trễ đáng kể trong việc xác nhận các sự kiện nhất định nào đó.
  + Nhiều host-based IDPS được thiết kế để chuyển cảnh báo đến server quản lý định kỳ, chứ không theo thời gian thực.
* Sử dụng tài nguyên của host: Hoạt động trên agent có thể làm chậm các hoạt động khác như kết nối mạng và sử dụng hệ thống file
* Xung đột với các cơ chế kiểm soát an ninh đang có: ví dụ personal firewall, nếu có các chức năng bị trùng lặp.

**Một số nền tảng HIDPS**

Hầu hết HIDPS sử dụng phần mềm trên host và một số chức năng quản lý bảo mật tập trung cho phép tích hợp với các dịch vụ theo dõi an ninh mạng và threat intelligence.

Ví dụ: Cisco AMP, AlienVault USM, Tripwire, Wazuh, và Open Source HIDS SECurity (OSSEC)

OSSEC sử dụng server quản lý trung tâm và các agents cài đặt trên các host riêng biệt.

**HIDPS: Ưu điểm và Nhược điểm**

Ưu điểm:

* Phát hiện các sự kiện trên hệ thống host, phát hiện thay đổi trong các file, bộ nhớ và ứng dụng.
* Có thể xử lý lưu lượng đã bị mã hoá (encrypted) để phát hiện các tấn công mà NIDS không thể phát hiện.
* Có thể so sánh các record lưu trong log theo dõi.

Nhược điểm:

* Thêm vấn đề quản lý, cần triển khai agent trên mỗi host muốn giám sát.
* Có thể chịu các tấn công trực tiếp hoặc tấn công vào host, dễ bị 1 số tấn công DoS.
* Cần một không gian ổ đĩa lớn, có thể ảnh hưởng đến hiệu suất của host.

**Chương 6**

Security monitoring – Giám sát an ninh. Cách gọi khác: Security Information Monitoring (SIM) hoặc Security Event Monitoring (SEM).

Bao gồm thu thập và phân tích thông tin để phát hiện các hành vi đáng ngờ hoặc các thay đổi hệ thống trái phép trên mạng, xác định loại hành vi nào nên được cảnh báo, và hành động cần thực hiện khi có cảnh báo.

**Giám sát các giao thức thông dụng**

**Syslog (System Logging Protocol)**

Syslog và Network Time Protocol (NTP) là các giao thức cần thiết cho hoạt động phân tích an ninh mạng

* Syslog là giao thức chuẩn dùng để gửi các log hệ thống hoặc các thông điệp sự kiện đến 1 server (server syslog), để ghi lại các sự kiện từ các thiết bị mạng và các thiết bị đầu cuối
* Server syslog thường lắng nghe trên port UDP 514 (cũng có thể dùng TCP)
* Các server syslog có thể trở thành mục tiêu bị tấn công
* Hacker có thể ngăn việc truyền và nhận dữ liệu, làm giả dữ liệu log hoặc giả mạo các phần mềm tạo và truyền log
* Một số cải tiến được cung cấp trong syslog-ng (next generation

**Network Time Protocol (NTP)**

Gói tin syslog thường được gán nhãn thời gian với giao thức Network Time Protocol (NTP)

* NTP hoạt động trên port UDP 123
* Nhãn thời gian rất quan trọng trong việc phát hiện tấn công
* Kẻ tấn công có thể tấn công vào NTP để làm gián đoạn thông tin thời gian dùng cho việc liên kết các sự kiện mạng đã được ghi log
* Kẻ tấn công có thể dùng các hệ thống NTP để chỉ đạo thực hiện tấn công DdoS

**DNS**

* Một số malware sử dụng DNS để giao tiếp với server command-and-control (CnC) và đánh cắp các dữ liệu được nguỵ trang dưới dạng các truy vấn DNS thông thường.
* Malware có thể mã hoá (encode) dữ liệu đánh cắp được trong phần subdomain trong truy vấn DNS cho 1 domain có nameserver đã bị kiểm soát bởi kẻ tấn công.
* Các truy vấn DNS với các tên domain được tạo ngẫu nhiên, hoặc các subdomain dạng chuỗi ngẫu nhiên rất dài đều đáng ngờ, đặc biệt nếu chúng xuất hiện với số lượng nhiều bất thường trong mạng.

**HTTP và HTTPS**

Các tấn công dựa trên web thường gồm các đoạn mã độc hại được cài vào webserver để chuyển hướng các trình duyệt client đến các server đã bị nhiễm thông quan việc load các iframe.

* Trong tấn công iFrame injection, kẻ tấn công chiếm 1 web server và cài mã độc tạo 1 iFrame ẩn trên các trang web thường được truy cập.
* Khi iFrame này được load trên trình duyệt của client, malware sẽ được tải về máy.

HTTPS có 1 lớp mã hoá (encryption) vào giao thức HTTP bằng cách sử dụng Secure socket layer (SSL)

**Các giao thức Email**

Các giao thức Email như SMTP, POP3, và IMAP

* SMTP gửi dữ liệu từ 1 host đến server mail và giữa các server mail, việc này không phải lúc nào cũng được giám sát.
* IMAP và POP3 thường được dùng để tải các email từ server mail về host và có thể dùng để tải các malware về host
* Giám sát an ninh có thể nhận dạng 1 malware dưới dạng file đính kèm đi vào mạng và xác định host nào sẽ bị ảnh hưởng đầu tiên

**ICMP**

* Có thể được dùng để xác định các host có trong mạng, kiến trúc của mạng, và xác định hệ điều hành sử dụng trong mạng,…
* Cũng có thể được dùng để thực hiện nhiều loại tấn công DoS
* ICMP cũng có thể được dùng để đánh cắp dữ liệu thông qua traffic ICMP từ bên trong mạng
* ICMP tunneling – Malware tạo các gói ICMP để truyền file từ host bị nhiễm đến kẻ tấn công

**Các công nghệ an ninh**

**ACLs**

ACLs có thể tạo ra 1 cảm giác sai về an toàn (false sense of security)

* Kẻ tấn công có thể xác định được các IP, giao thức và port nào được cho phép bởi ACL, thông qua các hoạt động như Port scanning, penetration testing, hoặc thông qua các hoạt động do thám mạng khác
* Kẻ tấn công có thể tạo các gói tin sử dụng địa chỉ IP nguồn giả mạo hoặc các ứng dụng có thể tạo kết nối với port bất kỳ

**NAT và PAT**

NAT (Network Address Translation) và PAT (Port Address Translation) có thể khiến việc giám sát an ninh mạng trở nên phức tạp

* Nhiều địa chỉ IP cùng được ánh xạ đến một hoặc nhiều địa chỉ IP công cộng sử dụng được trên Internet
* Ẩn các địa chỉ IP riêng bên trong mạng

**Mã hoá (Encryption) và Tunneling**

* Mã hoá (Encryption) là 1 phần trong hoạt động của Virtual Private Network (VPN) và HTTPS
* Kết nối ảo point-to-point giữa 1 host bên trong mạng và các thiết bị của kẻ tấn công
  + Malware có thể tạo 1 tunnel được mã hoá sử dụng các giao thức phổ biến và tin cậy, sau đó sử dụng tunnel này để đánh cắp dữ liệu từ mạng

**Mạng Peer-to-Peer và Tor**

Hoạt động mạng Peer-to-Peer

* Có thể phá vỡ biện pháp bảo vệ của tường lửa và thường là phương pháp phổ biến để lây lan malware.
* 3 dạng ứng dụng Peer-to-Peer: chia sẻ file, chia sẻ processor, và IM (tin nhắn)
* Các ứng dụng chia sẻ file P2P không nên cho phép hoạt động trong các mạng công ty

Tor là một nền tảng phần mềm và một mạng các host kết nối Peer-to-Peer hoạt động như các router trên mạng Tor

* Cho phép người dùng truy cập Internet ẩn danh bằng trình duyệt đặc biệt
* Có thể dùng che giấu danh tính kẻ tấn công và được dùng bởi các tổ chức tội phạm

Load Balancing – Cân bằng tải

Cân bằng tải là hoạt động phân phối lưu lượng mạng giữa các thiết bị hoặc đường mạng để tránh quá tải tài nguyên mạng

* Một số phương pháp cân bằng tải sử dụng DNS để gửi traffic đến tài nguyên có cùng tên domain nhưng nhiều địa chỉ IP
* Việc này có thể dẫn đến 1 kết nối Internet có thể được biểu diễn qua nhiều địa chỉ IP trong gói tin các đến

**Các loại dữ liệu an ninh**

**Dữ liệu Cảnh báo**

Dữ liệu Cảnh báo gồm các gói tin tạo ra từ các IDS/IPS khi có traffic vi phạm chính sách hoặc khớp với dấu hiệu của tấn công.

**Log trên thiết bị đầu cuối**

* Log của host: Host-based IDPS (HIDPS)
* Syslog
  + Gói tin Syslog gồm 3 phần: PRI (priority), HEADER, và MSG (nội dung dạng văn bản)
  + PRI gồm 2 phần, Facility và Severity của thông điệp
    - Facility gồm nhiều loại nguồn khác nhau tạo ra thông điệp đó như hệ thống, tiến trình, hoặc ứng dụng để chuyển gói tin đến file log tương ứng
    - Severity là 1 giá trị từ 0-7 xác định mức độ nghiêm trọng của thông điệp

A screenshot of a computer

Description automatically generated

* Log của Server
  + Server Email và Web có log truy cập (access) và log lỗi (error)
* Log truy cập (access) của Apache Webserver
  + Log truy cập của Apache Webserver ghi lại các request từ client đến server
  + 2 định dạng log
    - Common log format (CLF)
    - Dạng kết hợp: dạng CLF và thêm một số trường về referrer, user agent
* Log truy cập (access) của IIS
  + Microsoft IIS tạo các log truy cập có thể xem trên server với công cụ Event Viewer

**SIEM và Thu thập log**

Công nghệ Security Information and Event Management (SIEM)

* Hỗ trợ tạo báo cáo thời gian thực và phân tích dài hạn các sự kiện an ninh
* Các chức năng: Thu thập log, Chuẩn hoá, Tương quan sự kiện, Tích hợp, Báo cáo, Tuân thủ CNTT
* Một SIEM phổ biến là Splunk

**ELK** là từ viết tắt của 3 sản phẩm mã nguồn mở của Elastic:

* Elasticsearch: Công cụ tìm kiếm văn bản theo hướng tài liệu
* Logstash: như là 1 bộ tích hợp, thu thập và xử lý dữ liệu từ nhiều nguồn khác nhau trước khi đưa xuống pipeline
* Kibana: Dashboard phân tích và tìm kiếm cho Elasticsearch chạy trên trình duyệt
* Beats: một trong các công cụ chuyển log tốt nhất hiện nay, nhỏ gọn, hỗ trợ mã hoá, có cơ chế khôi phục tốt, đáng tin cậy

**SOC - Security Operations Center**

SOC là 1 vị trí trung tâm trong 1 doanh nghiệp, có các chuyên gia, quy trình và công nghệ để liên tục theo dõi và xử lý các vấn đề an ninh: phát hiện, phân tích, đánh giá, báo cáo và phản ứng với các vấn đề an ninh mạng.

Q: Điểm khác biệt giữa NOC và SOC?

* A: NOC là viết tắt của network operations center. NOC tập trung chủ yếu vào việc giảm thiểu thời gian downtime và đảm bảo các thoả thuận ở mức dịch vụ, trong khi SOC phân tích sâu hơn về các mối đe doạ mạng và các lỗ hổng

Q: Điểm khác biệt giữa SOC và SIEM?

* A: SIEM là viết tắt của Security Information and Event Management. SOC là 1 nhóm các chuyên gia và công cụ cùng làm việc chung với nhau và SIEM là một phần công việc họ cần tuân theo

**Chương 7**

Quản lý log – Log Management (LM) là hướng tiếp cận xử lý một số lượng lớn các log được tạo ra từ các thiết bị (cũng được gọi là audit record, audit trail, log sự kiện, v.v…).

LM bao gồm các chức năng thu thập log, tích hợp tập trung, lưu trữ lâu dài, phân tích log (theo real-time và theo nhóm sau khi lưu trữ) cũng như tìm kiếm log và tạo báo cáo.

SIEM (mô tả trong chương 6)

SIEM = phần mềm và dịch vụ bao gồm security information management (SIM) và security event management (SEM)

* SEM: giám sát thời gian thực, liên kết sự kiện, cảnh báo
* SIM: lưu trữ lâu dài, phân tích và báo cáo dữ liệu log

A blue and white text with black text

Description automatically generatedA screenshot of a computer

Description automatically generated

A triangle with different colors and text

Description automatically generatedA green and blue rectangles with black text

Description automatically generated

A diagram with text and arrows

Description automatically generated

A screenshot of a computer flowchart

Description automatically generated

**8 chức năng quan trọng của SIEM**

1. **Thu thập log**

* Thu thập log từ nhiều nguồn: Windows/Linux, ứng dụng, CSDL, router, switch,…
* Phương pháp thu thập log: agent-based hoặc agent-less
* Thu thập log tập trung
* Event Per Second (EPS) – tốc độ gửi sự kiện của hạ tầng CNTT
* Nếu không được tính toán phù hợp, SIEM có thể drop 1 số sự kiện trước khi lưu trên CSDL, dẫn đến các báo cáo, kết quả tìm kiếm, cảnh báo và tương quan không chính xác

1. **Giám sát hoạt động người dùng**

* SIEM cần giám sát hoạt động người dùng, quyền hạn người dùng và báo cáo giám sát
* Đảm bảo SIEM cung cấp “Complete audit trail” – truy vết đầy đủ
  + Biết user nào thực hiện hành động, kết quả của hành động, diễn ra trên server nào, thiết bị người dùng nào đã kích hoạt hành động, v.v

1. **Tương quan sự kiện thời gian thực**

* Hỗ trợ chủ động đối phó với các mối đe doạ
* Tăng bảo mật mạng bằng cách xử lý hàng triệu sự kiện đồng thời để phát hiện sự kiện đáng ngờ trên mạng
* Có thể dựa trên tìm kiếm log, các rule và cảnh báo
* Các rule và cảnh báo được định nghĩa trước không hiệu quả. SIEM cần hỗ trợ các trình tạo rule và alert tuỳ chỉnh
* Đảm bảo quá trình tương quan sự kiện thực hiện dễ dàng

1. **Lưu trữ log**

* Tự động lưu trữ tất cả dữ liệu log từ các hệ thống, thiết bị và ứng dụng vào 1 kho lưu trữ tập trung
* Cần đảm bảo tính năng Tamper Proof – mã hoá và gán nhãn thời gian log để phục vụ tuân thủ chính sách và điều tra pháp chứng
* Hỗ trợ truy xuất và phân tích log đã lưu

1. **Báo cáo tuân thủ chính sách:** Tuân thủ chính sách là cốt lõi của SIEM
2. **Giám sát tính toàn vẹn của file**

* SIEM cần giám sát và báo cáo tất cả thay đổi diễn ra như tạo, truy cập, xem, xoá, thay đổi, đổi tên file/thư mục, v.v
* SIEM cũng cần gửi các cảnh báo realtime khi có truy cập trái phép vào các file hoặc tập tin quan trọng

1. **Pháp chứng số trên log**

SIEM cần cho phép người dùng truy vết hành vi xâm nhập hoặc hoạt động của 1 sự kiện nào đó với khả năng tìm kiếm log

1. **Dashboard**

* Dashboard hỗ trợ quản trị viên thực hiện các hành động kịp thời và đưa ra quyết định cho các sự kiện đáng ngờ
* Dữ liệu an ninh cần được biểu diễn 1 cách trực quan và thân thiện với người dùng
* Dashboard cần hỗ trợ tuỳ chỉnh để quản trị viên có thể cấu hình các thông tin bảo mật cần quan sát

**Vì sao triển khai SIEM lỗi?**

Không có kế hoạch, Chiến lược triển khai lỗi, Vận hành thiếu giám sát, quản lý

A white paper with black text

Description automatically generated**Phân tích Xác định và Phân tích Xác suất**

Các kỹ thuật thống kê được dùng để đánh giá những rủi ro có thể xảy ra các tấn công trên 1 vùng mạng cho trước

* Phân tích xác định (Deterministic Analysis) – đánh giá rủi ro dựa trên những hiểu biết về một lỗ hổng
* Phân tích xác suất (Probabilistic Analysis) – ước tính khả năng một khai thác được thực hiện dựa trên khả năng của mỗi bước khai thác thành công

A white paper with black text

Description automatically generated

**Chương 8**

**Đánh lừa IDS - IDS evasion** là quá trình thay đổi các tấn công để đánh lừa IDS nhận diện thành các traffic hợp lệ và ngăn IDS tạo ra các cảnh báo.

1. **Insertion Attack**

* A green arrow pointing to a question mark

  Description automatically generatedLà quá trình kẻ tấn công lừa IDS đọc các gói tin không hợp lệ
* Xảy ra khi: NIDS có chính sách bảo vệ không chặt chẽ bằng hệ thống nội bộ
* IDS có thể chấp nhận những gói tin mà các hệ thống đầu cuối sẽ loại bỏ
* Tấn công nhằm thêm dữ liệu vào thông tin được đọc bởi IDS
* IDS nhận được nhiều gói tin hơn so với hệ thống đầu cuối

1. **Evasion**

* A close up of text

  Description automatically generatedỞ kỹ thuật này, hệ thống đầu cuối chấp nhận gói tin IDS chặn
* Kẻ tấn công có thể tấn công máy tính mà IDS không nhận ra
* Kẻ tấn công gửi các phần của yêu cầu tấn công trong các gói tin mà IDS sẽ chặn sai, cho phép bỏ đi 1 số phần của stream dưới góc nhìn của IDS
* IDS nhận ít gói tin hơn so với hệ thống đầu cuối

1. **Denial-of-Service Attack (DoS)**

* Nhiều IDS sử dụng server lưu trữ alert tập trung
* Kẻ tấn công có thể thực hiện DoS hoặc các tấn công khác vào server này để làm chậm hoặc crash server
* Khi đó, việc tấn công sau đó sẽ không bị ghi log

Với kỹ thuật qua mặt này, kẻ tấn công có thể:

1. Khiến 1 thiết bị bị khoá

2. Khiến cá nhân không thể điều tra tất cả các cảnh báo

3. Tạo ra nhiều cảnh báo cần được các hệ thống quản lý xử lý

4. Làm đầy không gian ổ cứng để không thể ghi log các tấn công

5. Tiêu tốn tài nguyên xử lý của thiết bị và từ đó có thể bỏ sót tấn công

1. **False Positive Generation**

* Kẻ tấn công có hiểu biết về IDS có thể tạo các gói tin độc hại chỉ để tạo ra các cảnh báo
* Những gói tin này được gửi đến IDS để tạo ra một lượng lớn các cảnh báo false positive
* Sau đó, kẻ tấn công lợi dụng những cảnh báo false positive này để che giấu traffic tấn công thực sự
* Kẻ tấn công có thể bypass qua IDS vì rất khó để phân biệt traffic tấn công với số lượng lớn các false positive
* Vấn đề
  + NIDS cần mô phỏng được hoạt động của các thiết bị đầu cuối và mạng nội bộ
  + Giới hạn về tài nguyên (CPU, bộ nhớ, bộ lưu trữ, băng thông)
  + NIDS thường hoạt động ở trạng thái “fail-open” – khi bị crash nó vẫn cho phép traffic đi qua để đảm bảo mạng vẫn hoạt động
* Một số dạng tấn công:
  + **DoS vào CPU** nhắm tới các hoạt động tiêu tốn tài nguyên tính toán (lắp ráp các fragment/segment, mã hoá/giải mã…)
  + **DoS vào bộ nhớ** nhắm tới các hoạt động quản lý trạng thái (TCP 3-way handshake, lắp ráp các fragment/segment…)
  + **DoS băng thông mạng** nhắm tới khiến NIDS không xử lý được gói tin đang truyền
  + **DoS hệ thống phản ứng**: tạo nhiều cảnh báo (false positive), chặn truy cập hợp lệ bằng cách giả mạo địa chỉ, che giấu tấn công thực

1. **Obfuscating – Làm rối mã**

* Trong kỹ thuật làm rối mã, kẻ tấn công encode payload tấn công ở dạng khác để chỉ có host đích decode được còn IDS thì không
* Một số ví dụ về kỹ thuật rối mã:
  + Kẻ tấn công có thể thay đổi đường dẫn được tham chiếu trong signature để đánh lừa HIDS
  + Kẻ tấn công có thể encode pattern tấn công trong Unicode để bypass bộ lọc của IDS, nhưng các Web server vẫn hiểu được
  + Code đa hình có thể qua mặt các signature-based IDS bằng cách tạo ra các pattern tấn công khác biệt, khi đó sẽ không có signature nào có thể phát hiện được tấn công
  + Các tấn công trong các giao thức được mã hoá như HTTPS cũng là 1 dạng làm rối mã

1. **Session Splicing**

* Kẻ tấn công chia nhỏ traffic tấn công thành nhiều gói tin để không 1 gói nào bật cảnh báo trên IDS
* Hiệu quả:
  + Có thể qua mặt các IDS không lắp ráp lại các gói tin trước khi kiểm tra chúng với các signature tấn công
  + Các tấn công session splicing thành công sẽ không bị ghi log trên IDS
  + Thêm delay giữa các gói tin được gửi để qua mặt quá trình lắp ráp gói tin trên IDS
    - Một số IDS ngừng lắp ráp nếu không nhận các gói sau 1 khoảng thời gian
    - Một số IDS ngừng hoạt động nếu có các session active lâu hơn thời gian lắp ráp
* Một số công cụ có thể thực hiện tấn công này: Nessus, Whisker
* Session Splicing với Whisker
  + Tấn công ở mức Network
  + Khác với IP fragmentation
  + Gửi các phần của request trong các gói tin khác nhau
  + "GET / HTTP/1.1" sẽ được chia thành nhiều gói tin thành dạng

"GE", "T ", "/", " H", "T", "TP", "/1", ".1"

* IP Fragmentations: Gói tin quá lớn đối với tầng data link, router có thể chia nhỏ thành nhiều fragment
* Session Splicing: Truyền payload qua nhiều gói tin một cách có mục đích để đánh lừa việc phát hiện tấn công - kích thước nhỏ hơn cần thiết
* Biện pháp đối phó
  + Fragment reassembly
  + Session reassembly
  + Send a reset [RST]

1. **Fragmentation Attack**

Fragmentation – Hoạt động phân mảnh có thể dùng để tấn công khi IDS và host có thời gian timeout cho việc phân mảnh khác nhau.

A screenshot of a computer

Description automatically generated

1. **Overlapping Fragments**

Overlapping Fragment – Phân mảnh chồng chéo: tạo ra loạt các fragment nhỏ với các sequence number chồng chéo nhau

Ví dụ: fragment đầu gồm 100 bytes payload với seq = 1, fragment thứ 2 có seq bị chồng có giá trị 96, v.v…

Khi lắp ráp lại gói tin, host đích cần biết cách lắp ráp các TCP fragment bị chồng chéo

* Một số OS như Windows W2K/XP/2003: giữ fragment gốc khi trùng seq
* Một số OS như Cisco IOS sẽ chọn các fragment đến sau có cùng seq

1. **Time-To-Live Attacks**

Attacker cần có hiểu biết trước về topology của mạng nạn nhân.

Sử dụng công cụ như traceroute để biết số router nằm giữa kẻ tấn công và nạn nhân.

Các bước tấn công:

A screenshot of a computer

Description automatically generated1. Attacker chia traffic thành 3 fragments

2. Kẻ tấn công gửi frag 1 với TTL cao, frag 2 giả với TTL thấp

3. IDS nhận cả 2 fragment, nhưng victim chỉ nhận fragment đầu

4. Kẻ tấn công gửi tiếp frag 3 với TTL cao

5. IDS lắp ráp 3 fragment thành 1 gói tin vô nghĩa và drop

6. Victim sau đó nhận frag 2 thật, và lắp ráp lại thành traffic tấn công, khi đó tấn công diễn ra nhưng không bị ghi log

1. **Invalid RST Packets**

Tấn công này dựa trên gói RST và giá trị checksum của nó:

* Cờ reset (RST) trong trường TCP được dùng để đóng 1 kết nối TCP
* TCP sử dụng trường checksum 16 bit để kiểm tra lỗi trong header và dữ liệu

Cách tấn công:

* Trong tấn công này, attacker gửi gói RST đến victim với giá trị checksum không hợp lệ
* IDS khi nhận gói RST nghĩ là TCP session đã kết thúc → IDS ngưng xử lý gói tin liên quan mặc dù victim vẫn sẽ nhận gói tin
* Victim kiểm tra checksum trong gói RST và drop nó
* Tấn công này cho phép attacker giao tiếp với victim trong khi IDS nghĩ rằng kết nối giữa 2 bên đã kết thúc

1. **Urgency Flag**

* Cờ Urgent (URG) trong TCP header được dùng để đánh dấu dữ liệu cần xử lý khẩn cấp tại host đích
* Nếu cờ URG được bật, giao thức TCP gán trường Urgent Pointer thành giá trị offset 16 bit trỏ đến byte cuối của dữ liệu khẩn cấp trong segment
* Nhiều IDS không xem xét urgent pointer và xử lý tất cả gói tin trong traffic trong khi victim chỉ xử lý dữ liệu khẩn cấp
* Điều này có thể khiến IDS và victim có tập gói tin khác nhau, có thể bị khai thác bởi attacker để gửi traffic tấn công
* Theo RFC 1122, urgency pointer sẽ khiến 1 byte dữ liệu nằm ngay sau dữ liệu khẩn cấp bị mất trong trường hợp kết hợp dữ liệu khẩn cấp và dữ liệu thường

1. **Unicode Evasion**

* Unicode là một hệ thống mã hoá ký tự nhằm hỗ trợ trao đổi, xử lý và hiển thị văn bản
* Trong mã Unicode, có thể có nhiều dạng biểu diễn khác nhau của cùng 1 ký tự
* Một số IDS có thể xử lý Unicode không chính xác
* Attacker có thể chuyển chuỗi tấn công sang dạng Unicode để qua mặt các phép so khớp pattern hay signature trên IDS
* Attacker có thể encode URL trong request HTTP với các ký tự Unicode để bypass phát hiện các tấn công web của IDS

1. **Polymorphic Shellcode – Đa hình**

* Nhiều IDS dựa trên signature sử dụng signature là những string thường được dùng trong các shellcode để phát hiện shellcode
* Tấn công shellcode đa hình bao gồm nhiều string shell code không cố định để gây khó khăn cho việc định nghĩa signature để có thể phát hiện tấn công
* Attacker encode payload với các kỹ thuật và đặt 1 decoder ở phía trước payload → shellcode được viết lại hoàn toàn mỗi lần nó được gửi đi để đánh lừa việc phát hiện
* Kỹ thuật này cũng qua mặt các string shellcode hay dùng, do đó, nó khiến các signature shellcode trở nên vô dụng.

1. **ASCII Shellcode**

* ASCII shellcode chứa các ký tự được biểu diễn trong chuẩn ASCII
* Attacker sử dụng ASCII shellcode để qua mặt các signature của IDS vì việc so khớp pattern không hoạt động hiệu quả với các giá trị ASCII
* Phạm vi của ASCII code có giới hạn vì không phải tất cả các lệnh assembly đều có thể chuyển trực tiếp sang các giá trị ASCII
* Giới hạn này có thể khắc phục bằng cách sử dụng tập các lệnh khác để có thể chuyển sang dạng ASCII

1. **Application-Layer Attacks**

* Các ứng dụng truy cập các file đa phương tiện (audio, video và hình ảnh) thường nén chúng thành các kích thước nhỏ hơn để tối đa hoá tốc độ truyền
* IDS không thể phát hiện signature của các dạng file đã nén
* Điều này có thể cho phép attacker khai thác lỗ hổng trong dữ liệu bị nén

1. **Desynchronization**

**Các dạng khác**

**Flooding**

Attacker gửi một loạt các traffic dư thừa để tạo ra traffic nhiễu, và nếu IDS không thể xử lý tốt traffic nhiễu thì traffic tấn công thực sự có thể sẽ không phát hiện được

Công cụ Traffic IQ Professional cho phép theo dõi và kiểm tra hoạt động của các thiết bị bảo mật bằng cách tạo ra các traffic ứng dụng chuẩn và traffic tấn công giữa 2 VM

A screenshot of a computer

Description automatically generated

**Vì sao cần Pentest IDS?**

* Kiểm ra IDS có đảm bảo thi hành **các policy IDS của tổ chức** hay không
* Kiểm tra IDS có đảm bảo thi hành **các policy bảo mật mạn**g hay không
* Kiểm tra IDS có đủ tốt để **ngăn chặn các tấn công từ bên ngoài**
* Kiểm tra hiệu quả của **vành đai bảo vệ mạng**
* Kiểm tra **lượng thông tin mạng có thể truy cập được** từ phía kẻ xâm nhập
* Kiểm tra **các nguy cơ bảo mật** có trên IDS có thể bị khai thác
* Đánh giá **tương quan giữa các rule IDS** và các hành động được thực hiện bởi chúng
* Kiểm tra policy bảo mật có **được thi hành chính xác** thông qua chuỗi các rule IDS hay không