



RESEARCH AND DEPLOY SIEM ON MICROSERVICES ENVIRONMENT

GVHD: ThS. Nguyễn Duy

Danh sách thành viên



Nguyễn Văn Tài
19522153

Nguyễn Trọng Tâm
19522164

NỘI DUNG

1. Giới thiệu

2. Kubernetes

3. Wazuh

4. DVWA

5. Mô hình

6. Demo



Giới thiệu





Giới thiệu

Tổng quan

Thông thường hệ thống CNTT trong doanh nghiệp được quản lý qua nhiều bộ phận như: mạng, ứng dụng, phần mềm,... Do đó, khi có sự cố xảy ra việc tổng hợp nhật ký và sự kiện trong thời điểm đó là rất khó. Quá trình điều tra nguyên do bị tấn công, nguồn tấn công sau đó tiêu tốn rất nhiều thời gian, công sức nhưng lại không đảm bảo hiệu quả.

Bên cạnh đó, các thủ đoạn tấn công ngày càng tinh vi mà các giải pháp bảo mật truyền thống hầu như không thể giúp ích trong việc chống trả lại.

Đó chính là lý do cần có giải pháp SIEM trong doanh nghiệp. Có SIEM mọi vấn đề phức tạp, rắc rối như trên sẽ được giải quyết.






Giới thiệu

SIEM - Security Information and Event Management

SIEM là hệ thống quản lý nhật ký và sự kiện tập trung, có nhiệm vụ thu thập thông tin nhật ký, sự kiện trong toàn hệ thống doanh nghiệp và tổng hợp tất cả trên 1 giao diện duy nhất thay vì phải làm thủ công từng cái một.

SIEM giúp thu thập tất cả nhật ký, sự kiện tập trung tại một chỗ để quản trị viên có thể phân tích chính xác vấn đề, phát hiện lỗi hỏng ở đâu từ đó đưa ra giải pháp xử lý. Có thể nói, hệ thống SIEM tương tự như cuốn từ điển ghi nhận lại tất cả sự việc trên hệ thống mạng nên có thể tra cứu thông tin bất kỳ lúc nào.

Các cảnh báo còn được đưa ra kịp thời nhằm tiết kiệm thời gian, nhân lực. Thậm chí, SIEM còn cung cấp cơ chế ngăn chặn tự động các cuộc tấn công mạng và ngắt kết nối với các thiết bị đã bị xâm hại để giảm thiểu tổn thất xuống mức thấp nhất.





Giới thiệu

Vấn đề

Từ đó, chúng tôi tìm hiểu và triển khai SIEM trên môi trường Microservices thông qua việc triển khai Wazuh trên môi trường Kubernetes.





Kubernetes



Kubernetes

Kubernetes là gì

Kubernetes (hay k8s) là một nền tảng open-source được dùng để quản lý container và được phát triển bởi Google. Có thể dùng kubernetes để phát triển ứng dụng trên nhiều nền tảng khác nhau như on-premise, cloud, or virtual machines.



kubernetes



Kubernetes

Lợi ích

Với kubernetes chúng ta có thể gom nhóm và quản lý container theo ứng dụng và project, nó cũng cung cấp các tính năng như Service Discovery and Load Balancing,...

Ngoài ra kubernetes còn nhiều tính năng khác như: auto scale resource, auto restart application when failure,...



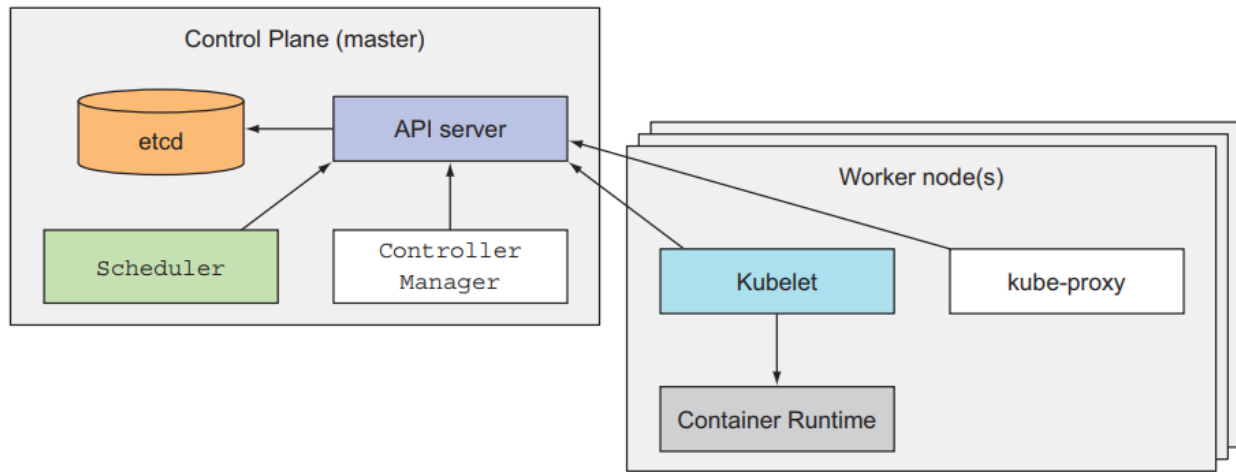
—

Kubernetes

Kiến trúc

Kubernetes cluster bao gồm 2 thành phần chính:

- Master nodes (control plane)
- Worker nodes





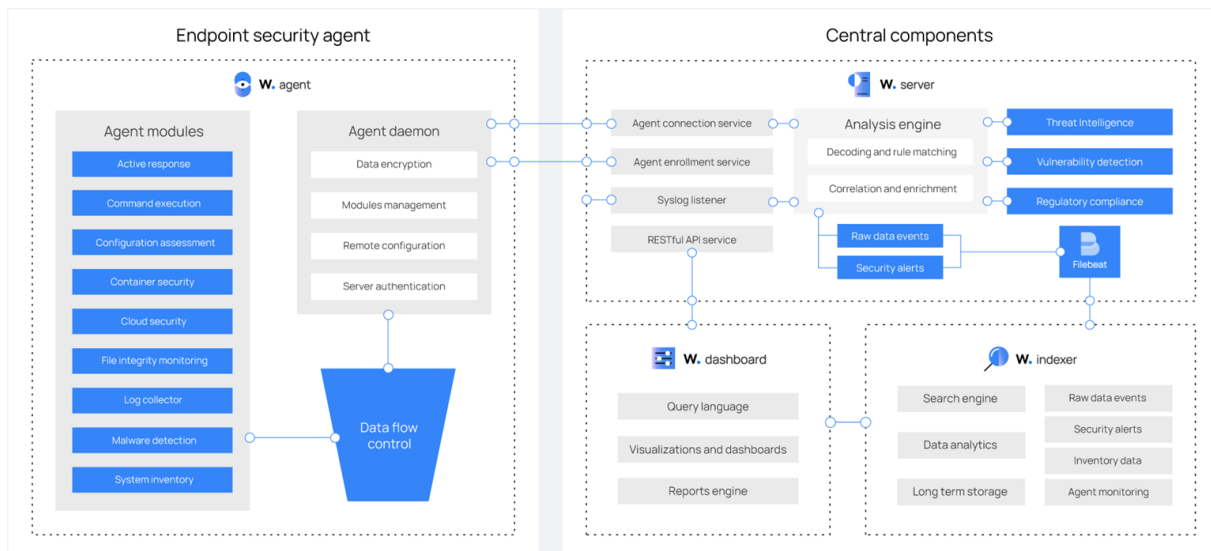
Wazuh



Wazuh

Tổng quan

Wazuh là một nền tảng bảo mật mã nguồn mở miễn phí hợp nhất các khả năng của XDR và SIEM. Nó bảo vệ khối lượng công việc trên các môi trường tại chỗ, ảo hóa, vùng chứa và dựa trên đám mây.



Wazuh

Khả năng của Wazuh

- Phát hiện xâm nhập
- Phân tích dữ liệu nhật ký
- Giám sát tính toàn vẹn tệp
- Phát hiện lỗi hỏng
- Đánh giá cấu hình
- Ứng phó sự cố
- Bảo mật đám mây
- Bảo mật container



~



Wazuh

Wazuh indexer

Wazuh indexer là một công cụ phân tích và tìm kiếm toàn văn bản có khả năng mở rộng cao. Nó lập chỉ mục và lưu trữ các cảnh báo do Wazuh server tạo ra, đồng thời cung cấp khả năng phân tích và tìm kiếm dữ liệu gần thời gian thực.





Wazuh

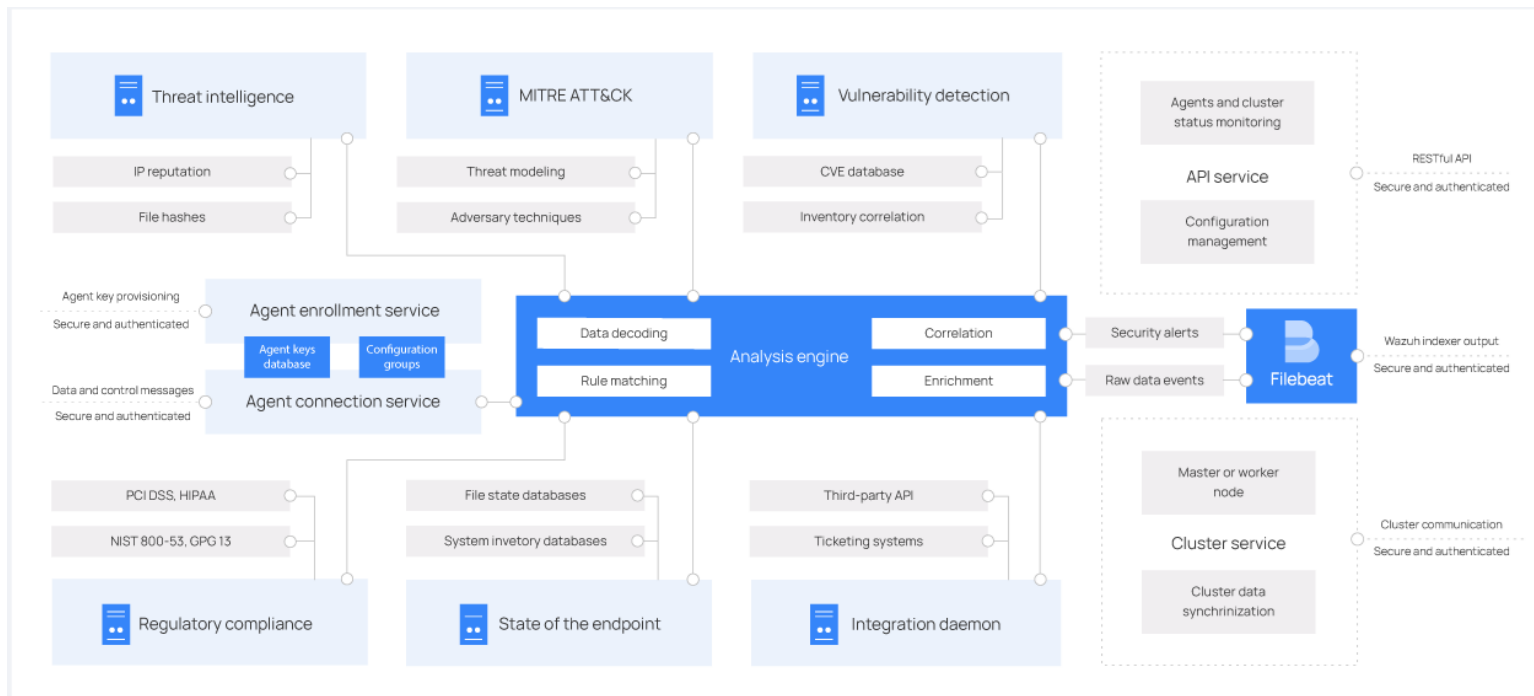
Wazuh server

Wazuh server phân tích dữ liệu nhận được từ các wazuh agent, kích hoạt cảnh báo khi phát hiện thấy các mối đe dọa hoặc sự bất thường. Nó cũng được sử dụng để quản lý cấu hình agent từ xa và theo dõi trạng thái của agent.



Wazuh server

Server architecture





Wazuh server

Server components

Analysis engine: Thực hiện phân tích dữ liệu. Nó sử dụng bộ giải mã để xác định loại thông tin đang được xử lý; sau đó, bằng cách sử dụng các quy tắc, công cụ xác định các mẫu cụ thể trong các sự kiện được giải mã; nó có thể kích hoạt cảnh báo và thậm chí có thể yêu cầu các biện pháp đối phó tự động.

Wazuh RESTful API: Dịch vụ này cung cấp giao diện để tương tác với cơ sở hạ tầng Wazuh. Nó được sử dụng để quản lý cài đặt cấu hình của các agent và server, theo dõi trạng thái cơ sở hạ tầng, quản lý và chỉnh sửa quy tắc và bộ giải mã Wazuh, đồng thời truy vấn về trạng thái của các điểm cuối được giám sát.





Wazuh server

Server components

Agent enrollment service: Nó được sử dụng để đăng ký đại lý mới. Dịch vụ này cung cấp và phân phối các khóa xác thực duy nhất cho mỗi tác nhân. Quá trình này chạy dưới dạng dịch vụ mạng và hỗ trợ xác thực qua chứng chỉ TLS/SSL hoặc bằng cách cung cấp mật khẩu cố định.

Agent connection service: Dịch vụ này nhận dữ liệu từ các đại lý. Nó sử dụng các khóa được chia sẻ bởi dịch vụ đăng ký để xác thực danh tính của từng tác nhân và mã hóa thông tin liên lạc giữa tác nhân Wazuh và máy chủ Wazuh. Ngoài ra, dịch vụ này cung cấp khả năng quản lý cấu hình tập trung, cho phép bạn đẩy cài đặt tác nhân mới từ xa.





Wazuh server

Server components

Wazuh cluster daemon: Dịch vụ này được sử dụng để mở rộng quy mô máy chủ Wazuh theo chiều ngang, triển khai chúng dưới dạng một cụm. Loại cấu hình này, kết hợp với bộ cân bằng tải mạng, mang lại khả năng sẵn sàng cao và cân bằng tải.

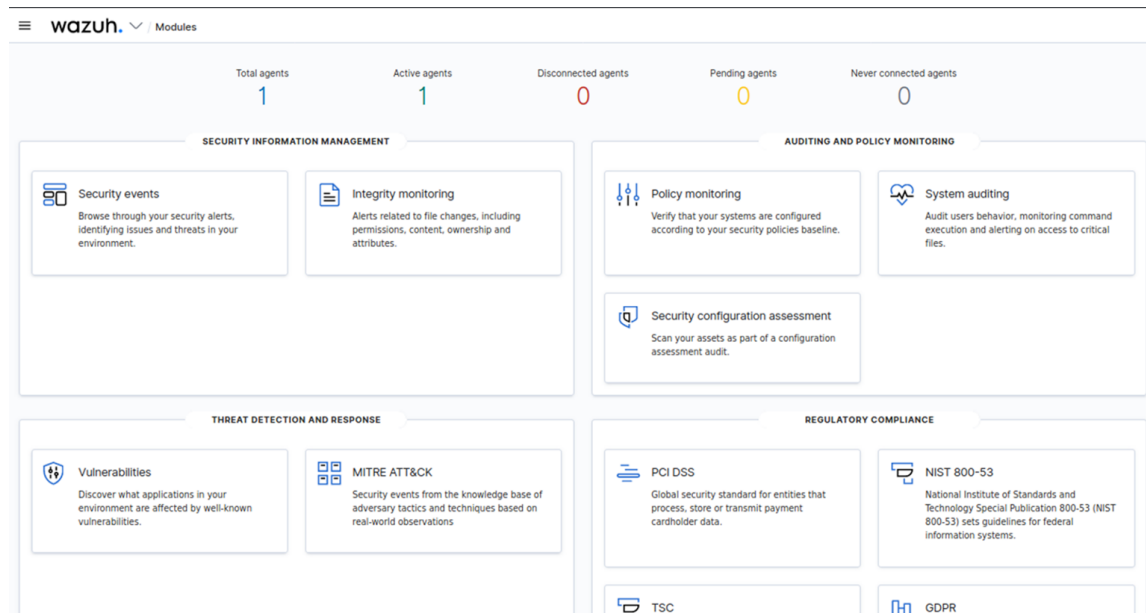
Filebeat: Nó được sử dụng để gửi các sự kiện và cảnh báo đến Wazuh indexer. Nó đọc đầu ra của Wazuh analysis engine và gửi các sự kiện trong thời gian thực. Nó cũng cung cấp khả năng cân bằng tải khi được kết nối với multi-node Wazuh indexer cluster.



Wazuh

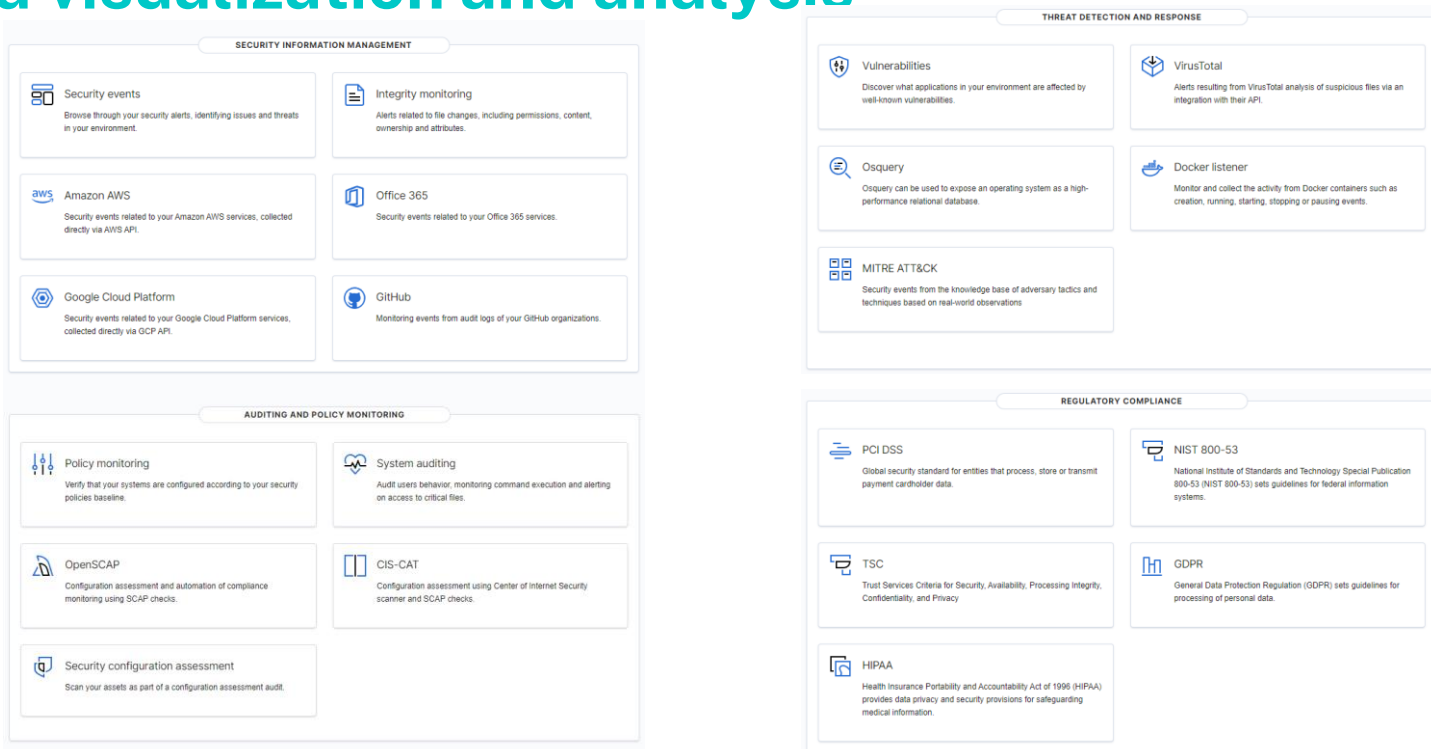
Wazuh dashboard

Thành phần trung tâm này là một giao diện web linh hoạt và trực quan để khai thác, phân tích và trực quan hóa dữ liệu bảo mật



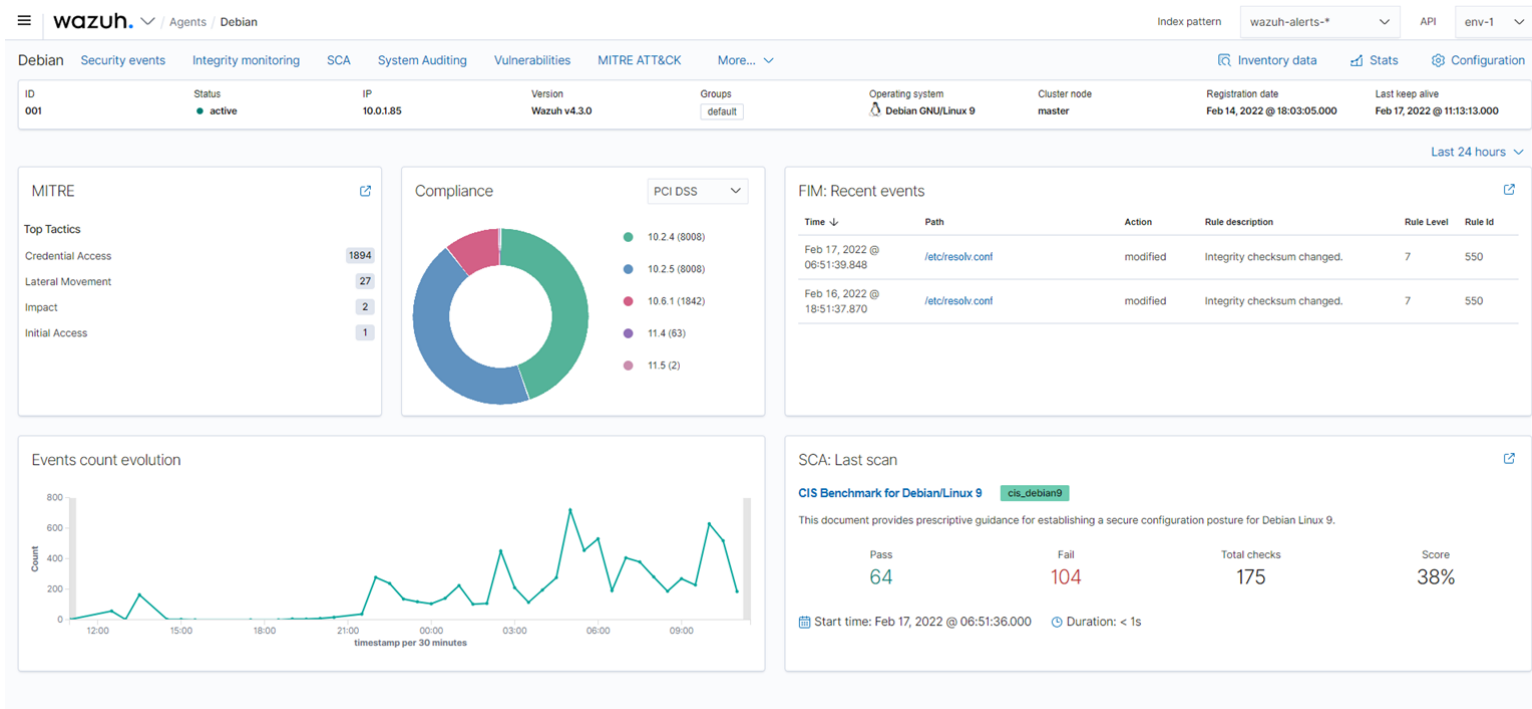
Wazuh dashboard

Data visualization and analysis



Wazuh dashboard


Agents monitoring and configuration





Wazuh dashboard


Platform management


ADMINISTRATION

**Rules**
Manage your Wazuh cluster rules.


**Decoders**
Manage your Wazuh cluster decoders.


**CDB lists**
Manage your Wazuh cluster CDB lists.


**Groups**
Manage your agent groups.


**Configuration**
Manage your Wazuh cluster configuration.


STATUS AND REPORTS

**Status**
Manage your Wazuh cluster status.

**Cluster**
Visualize your Wazuh cluster.

**Logs**
Logs from your Wazuh cluster.



**Reporting**
Check your stored Wazuh reports.


**Statistics**
Information about the Wazuh environment



Wazuh dashboard

Developer tools


 **wazuh.**  Ruleset Test

Index patternwazuh-alerts-*APIenv-1 

API Console Ruleset Test

Ruleset Test

Feb 18 17:01:22 linux-agent sshd[29205]: Invalid user blimey from 1.3.1.3 port 48928

 Clear session

```

**Phase 1: Completed pre-decoding.
  full event: Feb 18 17:01:22 linux-agent sshd[29205]: Invalid user blimey from 1.3.1.3 port 48928
  timestamp: Feb 18 17:01:22
  hostname: linux-agent
  program_name: sshd

**Phase 2: Completed decoding.
  name: sshd
  parent: sshd
  data: {
    "srcip": "1.3.1.3",
    "srcport": "48928",
    "srcuser": "blimey"
  }

**Phase 3: Completed filtering (rules).
  id: 5710
  level: 5
  description: sshd: Attempt to login using a non-existent user
  groups: ["syslog","sshd","authentication_failed","invalid_login"]
  firetimes: 1
  gdpr: ["IV_35.7.d","IV_32.2"]
  gpg13: ["7.1"]
  hipaa: ["164.312.b"]

```



Wazuh

Wazuh agent

Wazuh agent chạy trên Linux, Windows, macOS, Solaris, AIX và các hệ điều hành khác. Nó có thể được triển khai cho máy tính xách tay, máy tính để bàn, máy chủ, cloud instances, containers hoặc máy ảo.

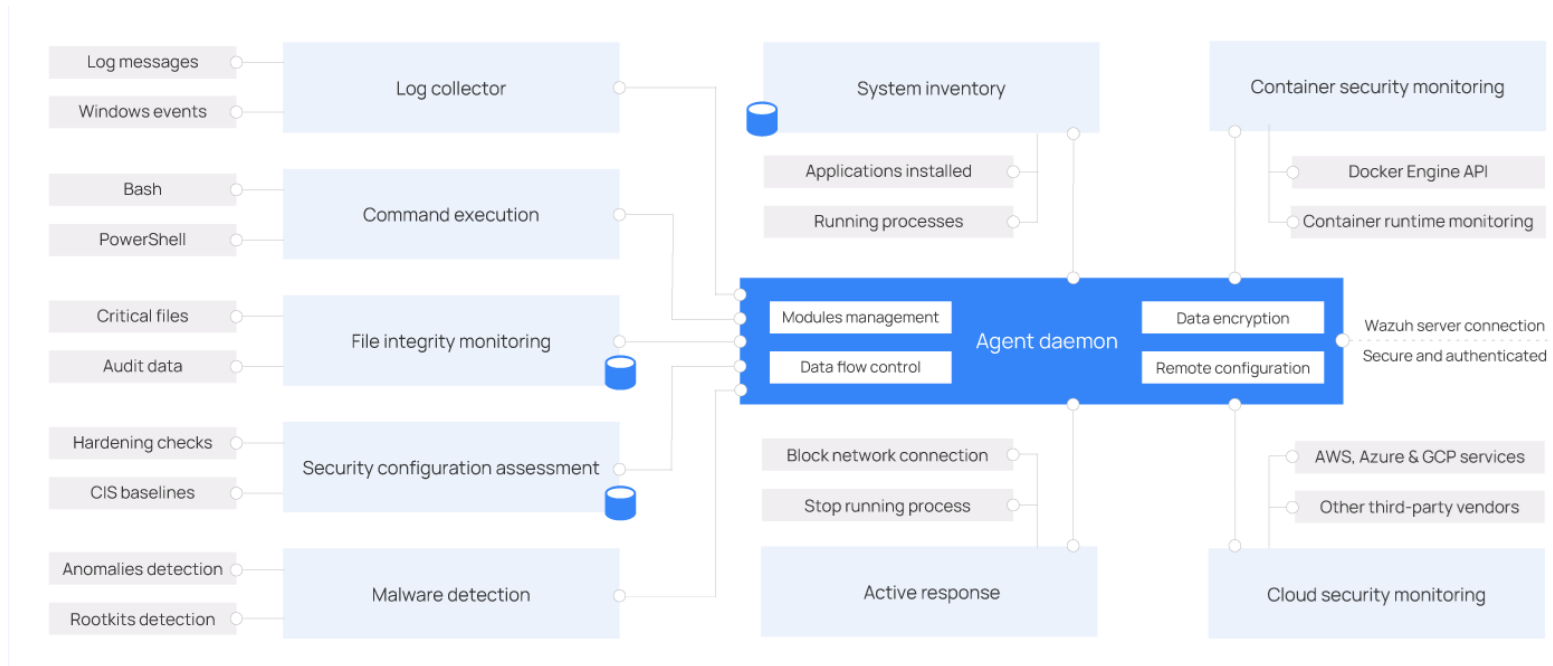
Agent cung cấp khả năng ngăn chặn, phát hiện và phản hồi mối đe dọa. Nó cũng được sử dụng để thu thập các loại dữ liệu ứng dụng và hệ thống khác nhau sau đó chuyển đến Wazuh server thông qua một kênh được mã hóa và xác thực.



Wazuh agent

Agent architecture

Wazuh Agent có kiến trúc mô-đun. Mỗi thành phần phụ trách các nhiệm vụ riêng.





Wazuh agent

Agent modules

Log collector: đọc các tệp flat log và các sự kiện Windows, thu thập các thông báo nhật ký của hệ điều hành và ứng dụng.

Command execution: Agents chạy các lệnh được ủy quyền theo định kỳ, thu thập đầu ra của chúng và báo cáo lại cho Wazuh server để phân tích thêm.

File integrity monitoring (FIM): giám sát hệ thống tệp.





Wazuh agent

Agent modules

Security configuration assessment (SCA): cung cấp đánh giá cấu hình bảo mật liên tục, sử dụng Center of Internet Security (CIS) benchmarks. Người dùng cũng có thể tạo kiểm tra SCA của riêng mình để theo dõi và thực thi các chính sách bảo mật.

System inventory: Scan định kỳ để thu thập dữ liệu kiểm kê như phiên bản hệ điều hành, giao diện mạng, các process đang chạy, ứng dụng đã cài đặt và danh sách các cổng đang mở. Kết quả quét được lưu trữ trong cơ sở dữ liệu SQLite cục bộ có thể được truy vấn từ xa.

Malware detection: Có khả năng phát hiện sự bất thường và sự hiện diện của rootkit. Ngoài ra, nó tìm kiếm các quy trình ẩn, tệp ẩn và cổng ẩn trong khi giám sát các system call.





Wazuh agent

Agent modules

Active response: Mô-đun này chạy các hành động tự động khi phát hiện thấy các mối đe dọa, kích hoạt các phản hồi để chặn kết nối mạng, dừng một quy trình đang chạy hoặc xóa một tệp độc hại.

Container security monitoring: Mô-đun tác nhân này được tích hợp với Docker Engine API để giám sát các thay đổi trong môi trường được chứa.

Cloud security monitoring: Thành phần này giám sát các nhà cung cấp đám mây như Amazon AWS, Microsoft Azure,...





DVWA

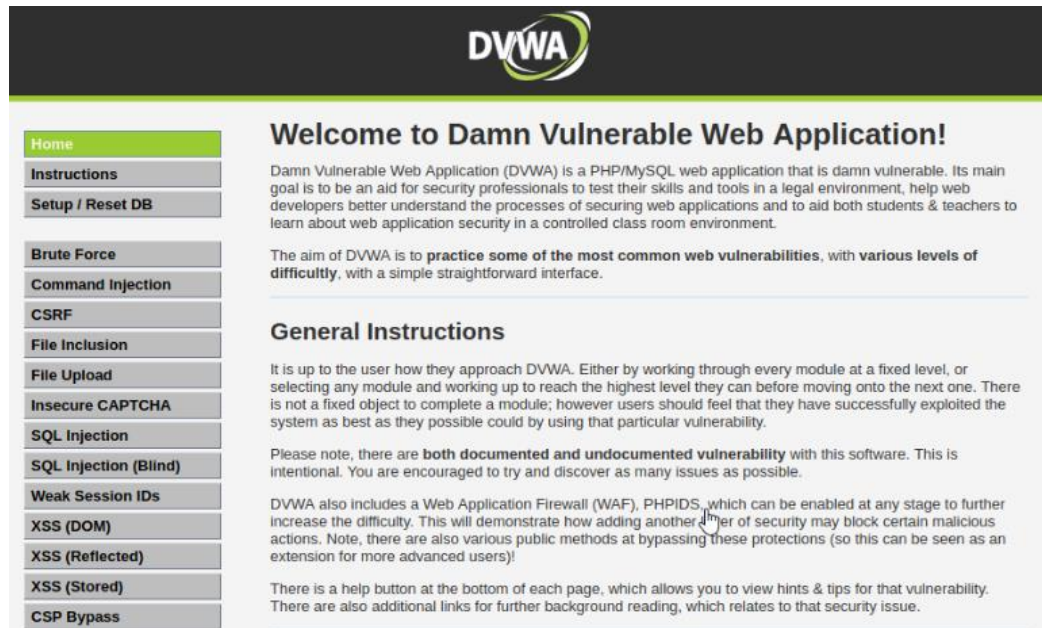


Damn Vulnerable Web Application

Giới thiệu

Damn Vulnerable Web Application (DVWA) là một ứng dụng mã nguồn PHP/MySQL tập hợp sẵn các lỗi logic về bảo mật ứng dụng web trong mã nguồn PHP.

Mục tiêu chính của DVWA đó là tạo ra một môi trường thực hành hacking/pentest hợp pháp. Giúp cho các nhà phát triển ứng dụng web hiểu hơn về hoạt động lập trình an toàn và bảo mật hơn.



The screenshot shows the DVWA homepage. At the top is the DVWA logo. Below it is a navigation menu with links: Home (highlighted), Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), and CSP Bypass. The main content area has a heading 'Welcome to Damn Vulnerable Web Application!' followed by a paragraph describing DVWA as a PHP/MySQL web application for security professionals. Below this is a section titled 'General Instructions' which explains the goal of the application and provides additional context about its features and usage.

DVWA

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another **layer** of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

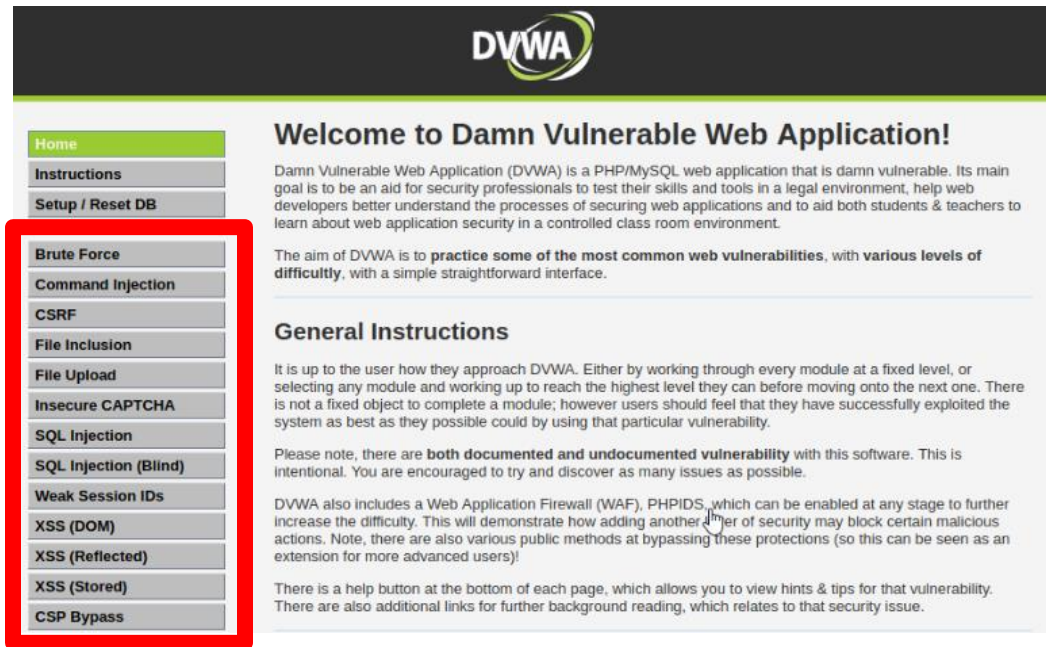
There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

Damn Vulnerable Web Application

Các lỗ hổng trong DVWA

Khi bạn thực hành với DVWA, ta sẽ có những nhóm lỗ hổng bảo mật sau:

- Brute Force
- Command Execution
- Cross Site Request Forgery (CSRF)
- File Inclusion
- SQL Injection
- Insecure File Upload
- Cross Site Scripting (XSS)
- Easter eggs



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another **layer** of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.



Damn Vulnerable Web Application

Các mức độ bảo mật

DVWA cung cấp 3 mức độ bảo mật tương ứng 3 level để bạn thực hành từ dễ cho đến khó gồm :

- **High** : level này gần như là level dùng để so sánh mã nguồn có lỗ hổng ở mức 'low' và 'medium' với mã nguồn đã được tối ưu ở mức an toàn bảo mật. Mức độ 'high' sẽ được đánh giá là có thể bao quát phần nhiều lỗ hổng ở nhóm mục bạn đang thực hành.
- **Medium** : mức độ này cung cấp nội dung logic code đã fix lỗ hổng cơ bản ở hạng mục mức 'low'.
- **Low** : mức độ thấp nhất trong thang level bảo mật mà DVWA cung cấp đến các bạn. Với mức độ 'low' thì mã nguồn PHP gần như phơi bày khả năng khai thác lỗ hổng qua tư duy lập trình chưa bao quát vấn đề bảo mật.

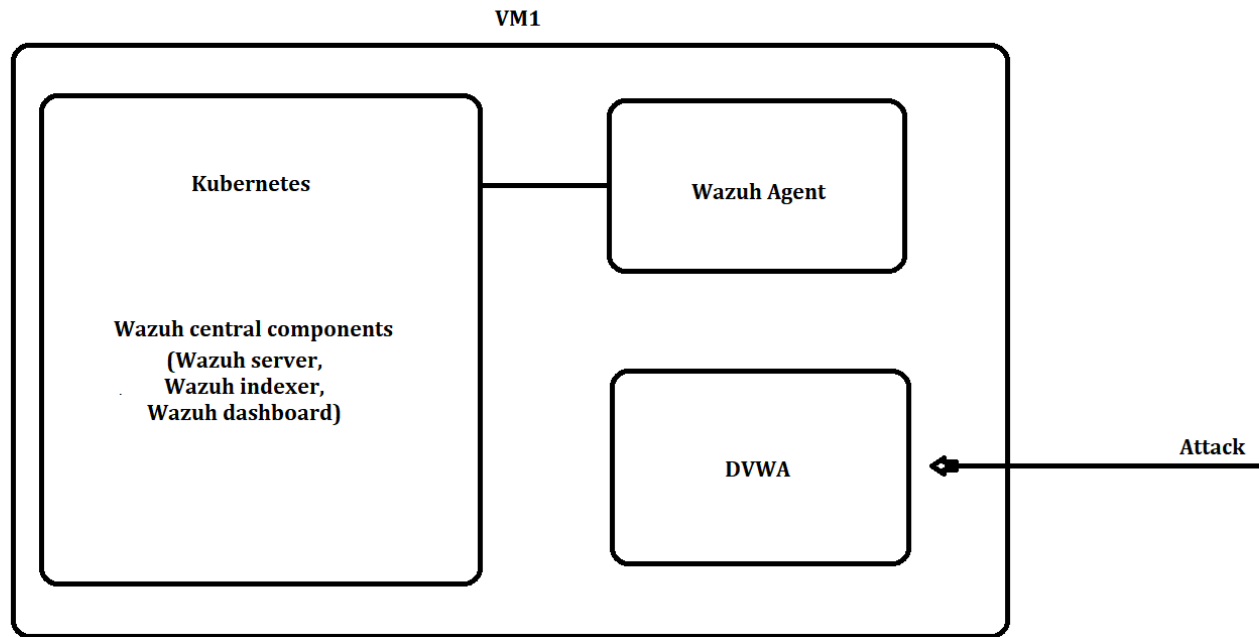




Mô hình



Mô hình





Demo



The image features a central text area surrounded by abstract geometric shapes. In the top-left corner, there are yellow and red circles, a pink textured shape, and a yellow curved line. The top-right corner shows a yellow and blue shape with a red dot. The bottom-left corner contains a yellow shape with red dots and a blue shape. The bottom-right corner features a pink shape, a red circle, and a yellow shape. The text is centered in a bold, blue, sans-serif font.

**THANKS FOR
WATCHING**