|  |  |  |
| --- | --- | --- |
|  |  |  |
| Firewall | Thiết bị hay phần mềm bảo mật đc sử dụng để kiểm soát lưu lượng đi qua nó . Nó có thể cho phép gói tin đi qua (accept) hoặc từ chối gói tin đó (reject) | -Hđ dựa trên rules : ip , nguồn ,port ,protocol  =>Accept or block |
| NG Firewall |  | -Nhiều hơn thế :   * 1.Deep packet inspection : sử dụng DPI , phân tích ứng dụng,ngữ cảnh và nội dung gói tin * 2.Intrusion prevention : tích hợp IPS * 3.SSL decryption : giải mã gói tin sử dụng mã hóa SSL để phân tích nội dung * 4.Identify User : có thể kiểm soát lưu lượng dựa trên danh tính người dùng * 5.Application awareness : xđ đc gói tin là của ứng dụng nào vd :lol,csgo,… |
| Web Apllication firewall | Firewall đặc biệt dành riêng cho ứng dụng web  -lọc,giám sát , block cái traffic HTTP/HTTPs . Inspect các data của các traffic này  =>>> | 1. Bảo vệ chống lại các cuộc tấn công trên ứng dụng web : XSS,CSRF,SQL Injection,..  2.Kiểm soát truy cập , xác thực  3.Phân tích : giám sát các hoạt động của user và attacker để phân tích và điều tra  4.Bảo vệ khỏi tấn công bot : dos ,Ddos,..=>. làm cho nó hđ hiệu quả  5.Tăng cường hiệu suất và độ tin cậy  6.Bảo vệ dữ liệu nhạy cảm sử dụng SSL/TLS |
| Database security | Biện pháp , quy trình bảo vệ CSDL khỏi các cuộc tấn công , lạm dụng và xâm nhập trái phép | 1. Giám sát,ghi logs 2. Quản lý quyền truy cập 3. Mã hóa dữ liệu 4. Giám sát ,kiểm tra , các hoạt động 5. Sao lưu và khôi phục |
| Next generation IPS | Cung cấp khả năng vượt trội so sánh với IPS truyền thống , đáp ứng vs các mối đe dọa ngày càng phức tạp và tiên tiến | 1. Phát hiện đc các cuộc tấn công mạng cụ thể (XSS,CSRF,SQL injection) 2. Phân tích chi tiết các gói tin mạng = DPI 3. Tích hợp thông tin từ nhiều nguồn để phân tích 4. Tích hợp SIEM 5. Tích hợp ML |
| Next generation Threat Protection | 1. Phát hiện , ngăn attacker hiện đại , tiến hóa 2. Tích hợp các cn bảo mật : IPS , firewall,Antimalware,virus ,…   3.Có tích hợp ML , sandbox,..  4.Anomaly-based detection.  5.Phù hợp vs mt phức tạp , linh hoạt , mở rộng tốt | 6.Đòi hỏi khả năng xử lý mạnh mẽ  7.Cần cập nhật liên tục |
| NG Endpoint Protection | Biện pháp , quy trình bảo mật đối với các thiết bị người dùng cuối như mt cá nhân , laptop ,.. | 1. Quản lí quyền truy cập 2. Phát hiện,ngăn malware : ML, AI,.. 3. Quản lí cấu hình bảo mật 4. Giám sát và phản ứng 5. Phục hồi và khôi phục |

**Đề tài 2 :Database Security : Data sunrise**

**A picture containing diagram, screenshot, design

Description automatically generated**

-**Data audit** : giám sát database theo thời gian thực , giám sát và ghi logs tất cả hoạt động liên quan đến database (user truy vấn , truy vấn gì , kết quả trả ra là gì ,…)

-Data security

-**Data masking** : mã hóa 1 số dữ liệu nhất định theo policies của admin , khi truy vấn thì dữ liệu đó sẽ không nhìn thấy được (vd : tk,mk của account , chỉ có số dư không được mã hóa)

-**Data discovery** : cho biết vị trí dữ liệu nhạy cảm (quan trọng) của họ nằm ở đâu trong database

-Compliance manager

-Vulnerability assessment

**Đề tài 3 : Security Incident Response Platform (The Hive)**

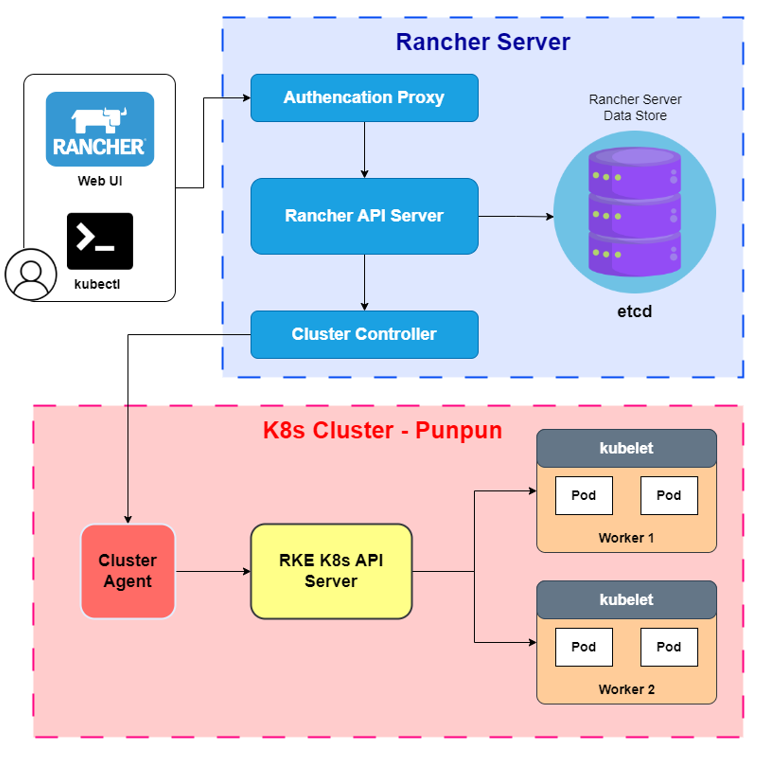
A picture containing text, screenshot, symbol, cartoon

Description automatically generated\

ShellShock attack:

Detect malware CDB-list:

**Đề tài 4 : Security features deployment for a Microservices Architecture**



Front-end : Html,node-js

Back-end:Python,Flask

Database :PostgreSQL,Redis

Rancher + kuctl : container

Neuvector : bảo vệ các ứng dụng web đc triển khai từ container

Calico : triển khai mạng -> kết nối các thành phần trong mạng lại với nhau

Cluster -> API server -> 2 Worker -> 2 pod/worker

**Đề tài 5 :Web Application Firewall Demonstration (ModSecurity)**

A picture containing text, screenshot, diagram, line

Description automatically generated

3 modes:

SecRuleEngine On :Bật tính năng bảo vệ ứng dụng web

SecRuleEngine DetectionOnly : Kiểm tra và ghi logs , không block traffic

SecRuleEngine OFF : không làm cái gì luôn

Demo attack:

1. SQL injection : truy vấn sql lấy data của CSDL
2. XSS injection (cross-site scripting) : lợi dụng vul và chèn JavaScript vào code HTML thông qua URL , khi user khác truy cập đến web thì sẽ load html đã bị thay đổi (vd : chèn link độc hại chuyển hướng user ,..)
3. File Upload Vulnerabilities : Hệ thống không kiểm tra file => upload file malware
4. Command Injection : Chèn command điều khiển hệ thống => chiếm quyền kiểm soát hệ thống,đọc ghi , xóa dữ liệu ,…
5. Password Brute force attack : dùng tool thử các password của các user từ cái 1 wordlist
6. Data theft : thay đổi URL đến các file trong trên máy triển khai webserver

**Đề tài 10 : Extended Detection Response Platform (WAZUH)**

3 thành phần :

-The Wazuh server : thu thập từ agents , xử lý events , quản lí cấu hình chung của hệ thống

-The wazuh indexer : tìm kiếm data trong wazuh server , phân tích , ktra lsu cua cac su kien bao mat

-The wazuh dashboard

Demo :

1. shellshock attacker
2. Detect malware – CBD list
3. Vuls Scan
4. File Integrity Monitoring
5. Monitor hidden running process