Project Akhir SIBKM Implementasi Pengamanan Web Server Menggunakan ModSecurity WAF dan OWASP CRS

Prerequisite:

Host Hardware:

- Min. 8 GB RAM
- Min. 100 GB Storage
- Hyper-V/Virtualization Support

Virtual Machine:

Web Server:

Akan bertindak sebagai Web Server dengan service Wordpress CMS.

App:

- PHP: 8.1
- MySQL: 8.0
- MariaDB: 10.5
- Apache HTTPD: 2.4
- Wordpress 6.7

VM:

- Min. 1 GB RAM (Min. 2 GB jika menggunakan GUI/Desktop Environment)
- Min. 1 Core CPU (Min. 1 GB jika menggunakan GUI/Desktop Environment)
- Min. 15 GB Storage
- Ubuntu 22.04 Server / Desktop OS

WAF Server:

Akan bertindak sebagai Reverse Proxy dan Web Application Firewall dari VM Web Server.

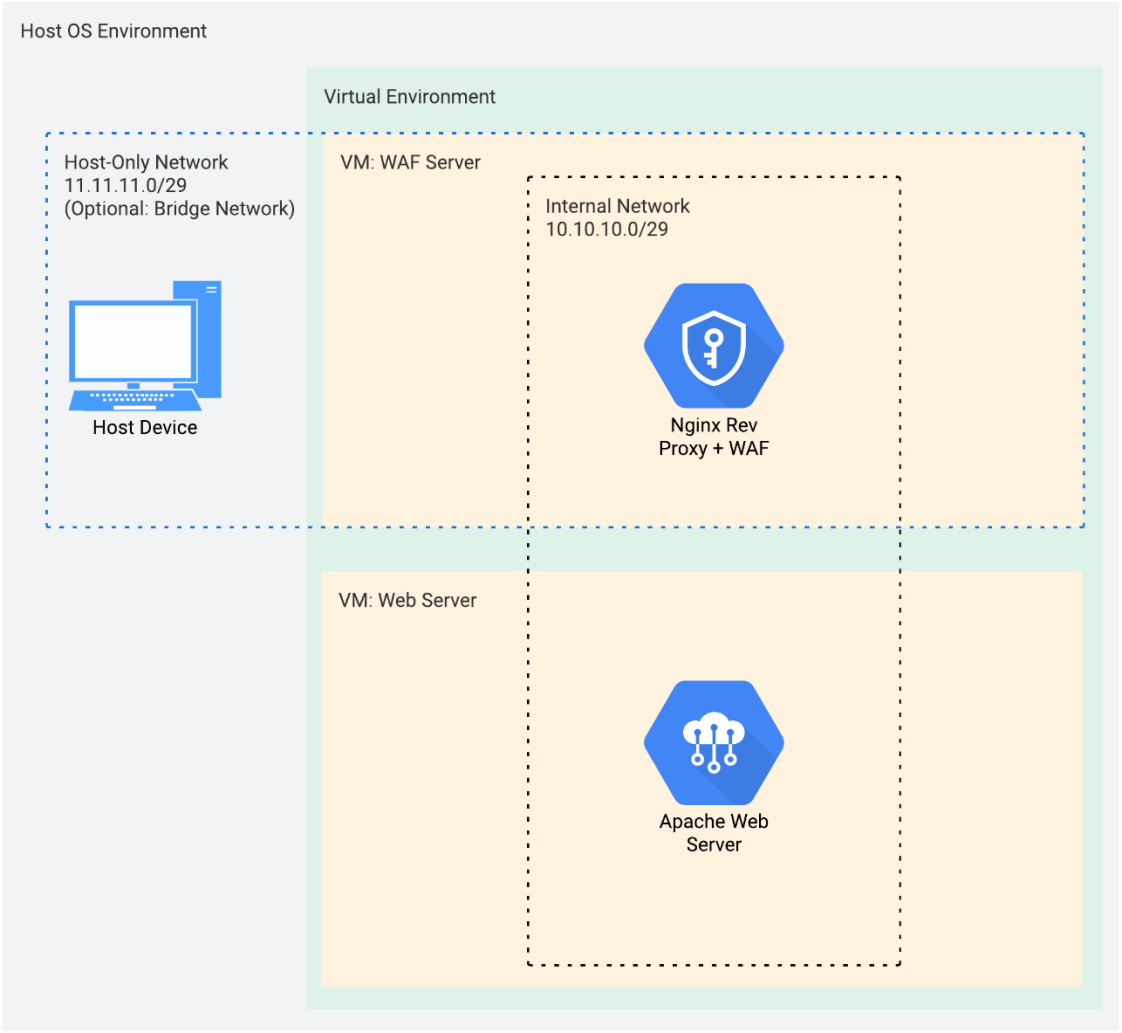
App:

- Nginx 1.24.0
- ModSecurity v3
- ModSecurity v3 Nginx Connector
- OWASP Core Rule Set

VM:

- Min. 1 GB RAM (Min. 2 GB jika menggunakan GUI/Desktop Environment)
- Min. 1 Core CPU (Min. 1 GB jika menggunakan GUI/Desktop Environment)
- Min. 15 GB Storage
- Ubuntu 22.04 Server / Desktop OS

Network / Environtment Architecture:



Gambar 1. Arsitektur Sistem

Scenario:

Pada project ini kita membuat lingkungan web server yang aman dengan melakukan segmentasi jaringan dan menerapkan beberapa security measure pada OS serta aplikasi atau service yang ada di dalamnya. Sesuai dengan arsitektur diatas, Web Server hanya dapat diakses melalui WAF Server yang bertindak sebagai WAF sekaligus reverse proxy untuk melindungi akses dari luar Internal Network. Lalu kita menggunakan CRS untuk menambah kapabilitas deteksi ancaman pada WAF dan melakukan pengujian serangan untuk memastikan bahwa WAF sudah bisa mendeteksi dan mencegah ancaman yang ada.

Assignment:

Host Device:

1. Lakukan installasi virtualization platform sesuai dengan platform pilihan.
2. Buatlah 2 virtual machine dengan spesifikasi yang sesuai.
3. Atur virtual network interface pada tiap virutal machine sesuai dengan arsitektur diatas:
    a. Host Device: Host-Only Network / Bridge Network
    b. WAF Server:

i. Interface 1: Host-Only Network / Bridge Network
ii. Interface 2: Internal Network

c. Web Server:
i. Interface 1: Internal Network

VM Web Server:

1. Lakukan installasi sistem operasi pada virtual machine.
2. Pastikan semua installation requirements sudah diinstall (MySQL, PHP, etc).
3. Lakukan installasi dan konfigurasi Apache2 sebagai web server.
4. Lakukan installasi dan konfigurasi Wordpress sebagai web application.
5. Pastikan wordpress berhasil diakses.

VM WAF Server:

1. Lakukan installasi sistem operasi pada virtual machine.
2. Lakukan installasi dan konfigurasi nginx sebagai reverse proxy yang dapat menerima dan meneruskan request dari/ke web application yang sudah di deploy pada VM Web Server.
3. Lakukan installasi dan konfigurasi ModSecurity v3 serta connector nya yang digunakan sebagai Web Application Firewall (WAF) untuk melindungi web application dari ancaman.
4. Lakukan installasi dan konfigurasi OWASP Core Rule Set (CRS) sebagai generic attack detection rules untuk menambah kapabilitas deteksi dari WAF.
5. Pastikan web application yang ada di VM Web Server dapat diakses melalui WAF Server.
6. Pastikan web application dapat diakses dari Host Device melalui WAF Server.

Final Step:

1. Lakukan pengujian terhadap WAF rules yang sudah diimplementasi dengan cara melakukan serangan / aktivitas malicious dari Host Device ke Web Server.
2. Pastikan serangan yang dilakukan terdeteksi dan berhasil dicegah oleh WAF.
3. Terapkan teknik security hardening sebanyak-banyaknya di masing-masing VM (dari segi OS, Application, etc) dan jelaskan fungsi dari masing-masing security measure yang diterapkan.
4. Buatlah file dokumentasi berupa laporan dari project ini dilengkapi dengan bukti tangkapan layar (screenshot) dari assignment yang dilakukan.

Note:

1. Format dokumen laporan:
    a. Cover
    b. Daftar Isi
    c. Ringkasan
    d. Hasil dan Pembahasan
        i. Host Machine
        ii. Web Server
        iii. WAF Server
        iv. Pengujian
        v. Hasil
    e. Penutup
    f. Referensi
    g. Dokumen Tambahan (Jika ada)

Referensi:

Berikut beberapa referensi yang mungkin dapat membantu:

- https://www.howtoforge.com/install-modsecurity-3-with-nginx-on-ubuntu-22-04/
- https://docs.nginx.com/nginx-waf/admin-guide/nginx-plus-modsecurity-waf-installation-logging/
- https://ioflood.com/blog/how-to-set-up-nginx-as-a-reverse-proxy-for-apache/
- https://modsecurity.org/
- https://github.com/owasp-modsecurity/ModSecurity-nginx
- https://github.com/owasp-modsecurity/ModSecurity/wiki/Compilation-recipes-for-v3.x
- https://www.f5.com/company/blog/nginx/compiling-dynamic-modules-nginx-plus
- https://coreruleset.org/docs/deployment/extended_install/index.html
- https://dev.to/henri_sekeladi/install-nginx-with-modsecurity-3-owasp-crs-on-ubuntu-2204-5d6l