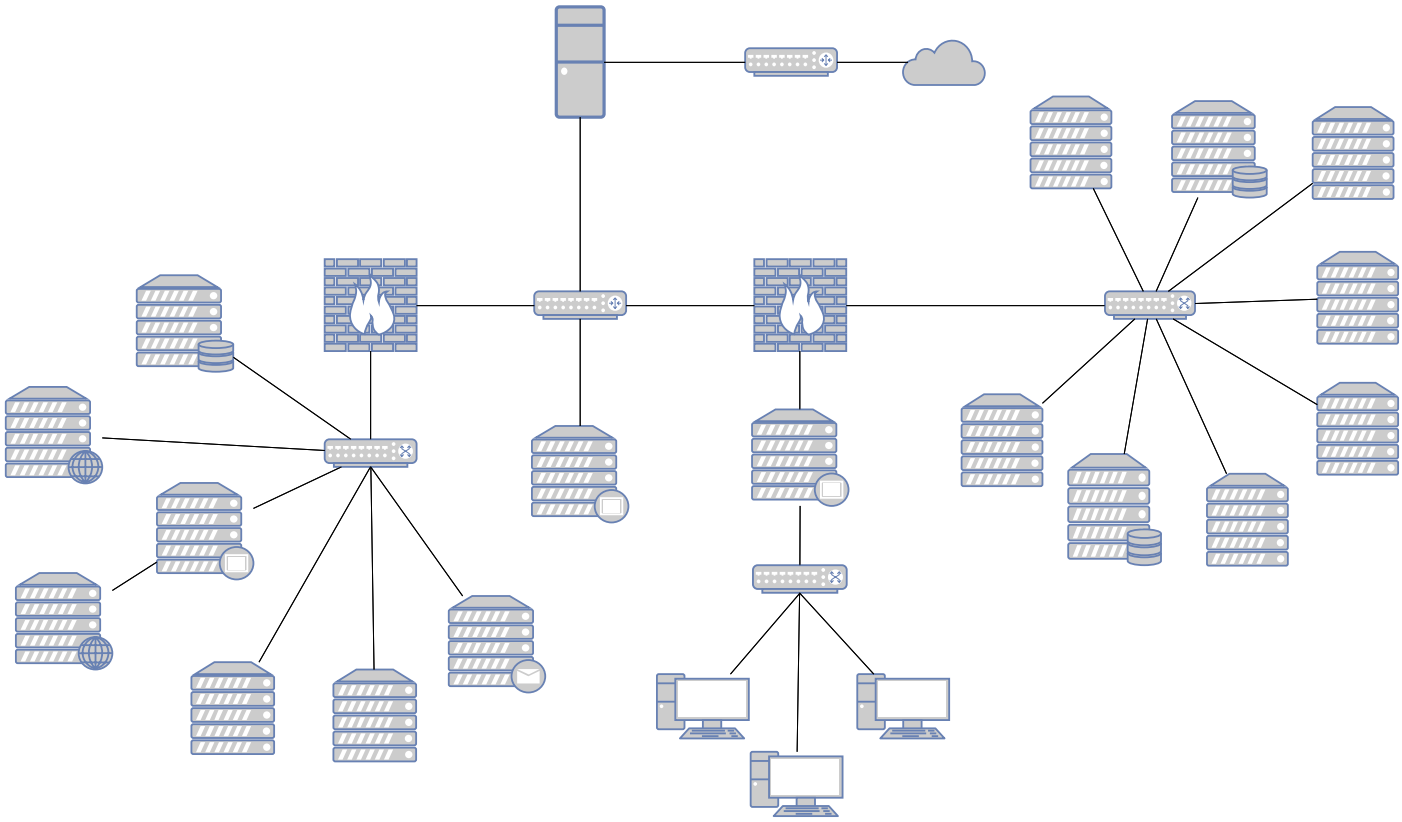
Escenario para Pentesting (II). Servicios desplegados (WIP)

2020-10-12

En este artículo se detallan los servicios que se van a usar junto con una pequeña descripción de los distintos niveles de madurez de estos. Estos niveles de madurez los vamos a clasificar como *basic*, *advanced* y *hardening*.



{:height=
width="100%"}

- DMZ Servers:
  - DB SQL (MariaDB)
  - DB NoSQL (MongoDB)
  - FTP (vsftpd)
  - Web Security Dojo
  - WAF (ModSecurity)
  - WEB (Apache2)
  - Monitorización (Nagios)
  - Almacenamiento (Owncloud)
  - Muña
  - Wordpress
  - Prestashop
  - Joomla
  - Drupal
  - Radius (freeradius)
  - DNS (bind9)
  - Honeypot (Cowrie)

    - Correo (Postfix)
- Router
    - firewall
    - VPN
    - IPv6
- IDS
- LAN Servers
    - VoIP (Asterisk)
    - LDAP (OpenLDAP)
    - SIEM (ELK)
    - SIEM (Splunk)
    - SIEM (EventLog Analyzer)
    - Active Directory
    - WEB (IIS)
    - Almacenamiento (SharePoint)
    - DB SQL (SQL Server)
    - ory/hydra OpenID
    - ory/hydra OAuth2
- LAN PCs
    - Windows XP
    - Windows 7
    - Windows 10

DMZ Servers

En esta subred se encuentran todos aquellos servicios que son alcanzables desde el exterior. Algunos de estos servicios tienes un acceso limitad a la subred interna de servidores, como por ejemplo para enviar los logs generados.

DB SQL (MariaDB)

Se usará MariaDB como base da datos SQL que almacena los datos de los siguientes servicios:

- Owncloud
- Asterisk
- Wordpress
- Prestashop
- Joomla

Basic

Está será la configuración que viene por defecto, con la excepción de que tiene que permitir conexiones desde cualquier IP, ya que será usada por servicios que tienen distintas IPs y que tendrá habilitada la auditoria para poder enviar.

Advanced

Está configuración tendrá mayores medidas de seguridad, como limitar el acceso por IP únicamente a los servicios que necesitan acceso a la base de datos.

Hardening

Esta configuración será mucho más avanzada, se usará la guía del CIS para hardenizar la base de datos.

//TODO Poner url pdf cis mysql

DB NoSQL (MongoDB)

//TODO ver el uso que se le da

Basic

Advanced

Hardening

FTP (vsftpd)

Se usará vsftpd como servidor FTP de la organización para la descarga de datos.

Basic

Está será la configuración que viene por defecto.

Advanced

Está configuración tendrá mayores medidas de seguridad, como pueden ser:

- Usar un servicio LDAP para la gestión de usuarios
- Usar únicamente FTPS (FTP over SSL) o SFTP (SSH File Transfer Protocol)
- Usar algún servicio como fail2ban para evitar ataques de fuerza bruta.

Hardening

Esta configuración será mucho más avanzada, se usará la guía del CIS para hardenizar el servicio.

Web Security Dojo

Web Security Dojo es un entorno de aprendizaje autónomo de código abierto para pruebas de penetración de seguridad de aplicaciones web, cuyos objetivos son:

- OWASP's WebGoat
- Google's Gruyere
- Damn Vulnerable Web App
- Hacme Casino
- OWASP InsecureWebApp
- w3af's test website
- simple training targets by Maven Security (including REST and JSON)

WAF (ModSecurity)

ModSecurity es un firewall de aplicaciones Web (WAF) embebible que se ejecuta como un módulo del servidor web Apache, provee protección contra diversos ataques hacia aplicaciones Web y permite monitorizar tráfico HTTP.

\TODO Investigar si tiene que estar como server proxy inverso o puede estar con el Apache junto con el resto de servicios (Menos consumo de recursos)

Basic

No va a estar configurado y únicamente redireccionará todas las peticiones HTTP al su respectivo servidor web

Advanced

Se va a configurar con el objetivo de que sea capaz de evitar SQL Injection y otros tipos de ataques web.

Hardening

Esta configuración será mucho más avanzada, se usará la guía del CIS para hardenizar el servidor web.

WEB (Apache2)

Se va a usar el servidor web Apache para desplegar una serie de servicios y CMS como son:

- Muña
- Nagios

- Owncloud
- Muña
- Wordpress
- Prestashop
- Joomla
- Drupal
- WebGoat
- phpmyadmin

Además se van a probar diferentes configuraciones de Apache para poner determinadas partes de una web con contraseña o usar el nuevo protocolo QUIC – HTTP/3.

Basic

Está será la configuración que viene por defecto, con la excepción de que se crearán virtualhost para cada una de las aplicaciones que se van a levantar usando Apache.

Advanced

Esta configuración hará uso de SSL y de certificados generados y firmados por una CA auto-firmada.

Hardening

Esta configuración será mucho más avanzada, se usará la guía del CIS para hardenizar el servidor web.

Monitorización (Nagios)

Se va a usar este servicio par monitorizar el funcionamiento de todos los hosts de la arquitectura, usando el protocolo SNMP, por lo que todos tendrán que tener configurado este protocolo.

Basic

Está será la configuración que viene por defecto, utilizando SNMPv2 para la monitorización de los hosts.

Advanced

Esta configuración hará uso de un certificado para cifrar las comunicaciones. Además que se cambiara SNMPv2 por SNMPv3 para que el tráfico de monitorización vaya cifrado.

Hardening

\TODO

Almacenamiento (Owncloud)

Basic

Advanced

Hardening

Muña

Muña es una aplicación vulnerable cuyo objetivo es practicar seguridad y hacking ético de aplicaciones y servicios web.

Permite practica como atacar usando técnicas como inyección SQL, XSS, exposición de Recursos, exposición de Credenciales, seguridad de Base de Datos, etc.

También permite aprender como defenderte escribiendo código seguro y otras formas de prevención para las aplicaciones.

Basic

Está será la configuración que viene por defecto.

Advanced

Está configuración se realizará tras un análisis del código y realizando la programación necesaria para securizar la aplicación web y eliminar las vulnerabilidades detectadas en la fase anterior.

Wordpress

Basic

Advanced

Hardening

Prestashop

Basic

Advanced

Hardening

Joomla

Basic

Advanced

Hardening

Drupal

Basic

Advanced

Hardening

Radius (freeradius)

Basic

Advanced

Hardening

DNS (bind9)

Basic

Advanced

Hardening

Honeypot (Cowrie)

Basic

Advanced

Hardening

Correo (Postfix)

Basic

Advanced

Hardening

Router

IDS

LAN Servers

VoIP (Asterisk)

LDAP (OpenLDAP)

SIEM (ELK)