MILLORNET

Empresa de Ciberseguridad y Pentesting

Documentacion Tecnica de Infraestructura

Proyecto Final ASIX
Curso 2025-2026

1. Introduccion

Millornet es una empresa simulada de ciberseguridad y pentesting montada sobre VirtualBox como proyecto final del ciclo ASIX. La infraestructura replica un entorno empresarial real con segmentacion de redes, servicios en contenedores Docker, monitorizacion, backups y herramientas de pentesting.

El objetivo del proyecto es demostrar la capacidad de disenar, desplegar y gestionar una infraestructura de red profesional, incluyendo un router con multiples funciones, un servidor principal con stack de servicios Docker, una DMZ con servicios expuestos y una red de laboratorio para pruebas de pentesting.

2. Arquitectura de Red

2.1 Diagrama de Red

La infraestructura de Millornet esta compuesta por 4 redes diferenciadas:

Red	Subred	Interfaz Router	Descripcion
WAN	192.168.1.0/24	enp0s3 (Puente)	Salida a internet
Empresa	10.10.10.0/24	enp0s8	Red interna corporativa
DMZ	10.20.20.0/24	enp0s9	Servicios expuestos al exterior
Laboratorio	10.30.30.0/24	enp0s10	Red de victimas para pentesting

2.2 Politica de Segmentacion

Las redes estan segmentadas con las siguientes politicas de acceso:

Origen	Destino	Permitido	Justificacion
Empresa	Internet	Si	Acceso total a internet
Empresa	DMZ	Si	Gestion de servicios DMZ
Empresa	Laboratorio	Si	Lanzamiento de ataques pentesting
DMZ	Internet	Si	Servicios web/mail necesitan salida
DMZ	Empresa	No	Aislamiento de seguridad
DMZ	Laboratorio	No	Aislamiento de seguridad
Laboratorio	Internet	No	Contencion de maquinas vulnerables

Origen	Destino	Permitido	Justificacion
Laboratorio	Empresa	No	Evitar pivoting desde victimas
Laboratorio	DMZ	No	Evitar pivoting desde victimas

2.3 Inventario de Maquinas Virtuales

VM	Hostname	IP Empresa	IP Host-Only	Rol
Router	millornet-router	10.10.10.1	192.168.1.39	Router, DNS, DHCP, Firewall, VPN
Servidor	millornet-server	10.10.10.10	192.168.56.102	Docker, Portainer, Grafana, Backups
DMZ	millornet-dmz	10.20.20.10	192.168.56.103	Nginx, Mailserver, FTP
Laboratorio	millornet-lab	10.30.30.x	-	Contenedores vulnerables (DVWA, etc.)

3. Router Millornet

El router esta basado en Ubuntu Server 24.04 LTS y actua como nucleo de la red Millornet, gestionando el enrutamiento entre todas las redes, los servicios de red basicos y la seguridad perimetral.

3.1 Servicios del Router

Servicio	Software	Funcion
NAT / Enrutamiento	iptables + ip_forward	Permite salida a internet a las redes internas
DHCP	isc-dhcp-server	Asignacion automatica de IPs en las 3 redes
DNS	Bind9	Resolucion de nombres internos y forwarding externo
Firewall	iptables (script)	Segmentacion y control de trafico entre redes
VPN	WireGuard	Acceso remoto seguro a la red interna
Monitorizacion	ntopng + iftop	Analisis de trafico en tiempo real
Proteccion SSH	Fail2ban	Bloqueo automatico de ataques de fuerza bruta

3.2 DNS - Zonas Configuradas

Zona	Tipo	Registros principales
millornet.local	Master	router (10.10.10.1), server (10.10.10.10)
dmz.millornet.local	Master	router (10.20.20.1), dmz (10.20.20.10), www, mail, ftp
lab.millornet.local	Master	router (10.30.30.1), victima1 (10.30.30.10)

3.3 DHCP - Rangos por Red

Red	Rango DHCP	Gateway	DNS
millornet.local	10.10.10.10 - 10.10.10.100	10.10.10.1	10.10.10.1
dmz.millornet.local	10.20.20.10 - 10.20.20.50	10.20.20.1	10.20.20.1

Red	Rango DHCP	Gateway	DNS
lab.millornet.local	10.30.30.10 - 10.30.30.50	10.30.30.1	10.30.30.1

3.4 VPN WireGuard

WireGuard proporciona acceso remoto seguro a la infraestructura Millornet mediante tunel cifrado.

Parametro	Valor
Interfaz VPN	wg0
Red VPN	10.99.99.0/24
IP Servidor	10.99.99.1
IP Cliente	10.99.99.2
Puerto	UDP 51820
Redes accesibles	10.10.10.0/24, 10.20.20.0/24, 10.30.30.0/24

4. Servidor Principal - Stack Docker

El servidor principal ejecuta todos los servicios corporativos de Millornet mediante contenedores Docker gestionados con Docker Compose. Esto permite un despliegue reproducible, aislamiento de servicios y facilidad de mantenimiento.

4.1 Servicios Docker

Contenedor	Imagen	Puerto	Funcion
millornet-traefik	traefik:latest	80, 443, 8080	Proxy inverso y balanceador de carga
millornet-portainer	portainer/portainer-ce	9000	Panel de gestion de contenedores Docker
millornet-duplicati	linuxserver/duplicati	8200	Sistema de backups cifrados
millornet-prometheus	prom/prometheus	9090	Recoleccion de metricas del sistema
millornet-grafana	grafana/grafana	3000	Dashboard visual de monitorizacion
millornet-node-exporter	prom/node-exporter	9100	Exportacion de metricas del SO
millornet-cadvisor	gcr.io/cadvisor	8081	Metricas de contenedores Docker

4.2 Sistema de Backups (Duplicati)

Duplicati realiza backups automaticos diarios de toda la infraestructura Docker con cifrado AES-256.

Parametro	Valor
Nombre	Backup Millornet
Origen	/source (~/millornet)
Destino	/backups
Cifrado	AES-256
Frecuencia	Diario a las 2:00 AM
Retencion	7 versiones

4.3 Monitorizacion (Grafana + Prometheus)

El stack de monitorizacion permite visualizar en tiempo real el estado del servidor y los contenedores Docker.

Dashboard	ID Grafana	Metricas
Node Exporter Full	1860	CPU, RAM, disco, red, temperatura
Docker Containers	893	Estado, CPU y memoria de contenedores

5. DMZ - Servicios Expuestos

La DMZ (Zona Desmilitarizada) aloja los servicios que Millornet expone hacia el exterior. Estos servicios son accesibles desde la red empresa pero estan aislados de ella para minimizar el impacto en caso de compromiso.

5.1 Servicios DMZ

Contenedor	Imagen	Puerto	Dominio	Funcion
dmz-nginx	nginx:latest	80, 443	www.dmz.millornet.local	Web corporativa de M
dmz-mailserver	docker-mailserver	25, 587, 993	mail.dmz.millornet.local	Servidor de correo el
dmz-ftp	garethflowers/ftp-server	20, 21	ftp.dmz.millornet.local	Servidor FTP corpora

5.2 Web Corporativa

El servidor web Nginx sirve la pagina corporativa de Millornet accesible en http://www.dmz.millornet.local. La pagina presenta los servicios de ciberseguridad y pentesting de la empresa.

6. Red de Laboratorio - Pentesting

La red de laboratorio (10.30.30.0/24) esta completamente aislada del resto de la infraestructura. En ella se despliegan maquinas vulnerables para realizar pruebas de pentesting de forma segura y controlada.

6.1 Contenedores Vulnerables Planificados

Contenedor	Imagen	Vulnerabilidades	Objetivo
DVWA	vulnerables/dvwa	SQL Injection, XSS, CSRF, File Upload	Practica de pentesting web
WebGoat	webgoat/goat-and-wolf	OWASP Top 10	Formacion en seguridad web
Juice Shop	bkimminich/juice-shop	Multiples vulnerabilidades OWASP	CTF y pentesting avanzado
Metasploitable	tleemcjr/metasploitable2	Multiples servicios vulnerables	Practica con Metasploit

6.2 Metodologia de Pentesting

Las pruebas de pentesting seguiran la metodologia estandar del sector:

- Reconocimiento: Escaneo de puertos y servicios con Nmap
- Enumeracion: Identificacion de versiones y vulnerabilidades con Nessus/OpenVAS
- Explotacion: Uso de Metasploit Framework y herramientas especificas
- Post-explotacion: Escalada de privilegios y movimiento lateral
- Reporte: Documentacion de hallazgos y recomendaciones

7. Medidas de Seguridad

Medida	Herramienta	Descripcion
Segmentacion de red	iptables	Cada red aislada con politicas de acceso estrictas
Firewall perimetral	iptables (script)	Reglas DROP por defecto, solo se permite lo necesario
Proteccion SSH	Fail2ban	Banea IPs tras 3 intentos fallidos durante 2 horas
VPN	WireGuard	Acceso remoto cifrado con claves asimetricas
Backups cifrados	Duplicati + AES-256	Copias de seguridad diarias con cifrado fuerte
Monitorizacion	ntopng + Grafana	Deteccion de anomalias en el trafico de red
Acceso SSH restringido	iptables	SSH al router solo desde red empresa (10.10.10.0/24)

8. Guia de Acceso a los Servicios

8.1 Acceso via SSH Tunnel

Para acceder a los paneles web desde el PC principal se utiliza SSH tunneling:

Tunel al servidor principal:

```
ssh -L 9000:10.10.10.10:9000 -L 3000:10.10.10.10:3000 -L 8080:10.10.10.10:8080 -L 8200:10.10.10.10:8200 ikervp@192.168.56.102
```

Tunel a la DMZ:

```
ssh -L 8888:10.20.20.10:80 ikervp@192.168.56.103
```

8.2 URLs de Acceso

Servicio	URL Local (SSH Tunnel)	Credenciales
Portainer	http://localhost:9000	admin / (configurado al instalar)
Grafana	http://localhost:3000	admin / Millornet2026!
Traefik Dashboard	http://localhost:8080	Sin autenticacion
Duplicati	http://localhost:8200	alumnes
Web DMZ	http://localhost:8888	Publica
ntopng Router	http://192.168.1.39:3000	admin / admin

9. Planes a Futuro

La infraestructura Millornet esta en continuo desarrollo. A continuacion se detallan las mejoras y ampliaciones planificadas para completar el proyecto:

9.1 Red de Laboratorio - Maquinas Vulnerables

El siguiente paso es desplegar la red de laboratorio con contenedores Docker vulnerables:

- Despliegue de DVWA (Damn Vulnerable Web Application)
- Instalacion de WebGoat para practica de OWASP Top 10
- Configuracion de OWASP Juice Shop para CTF
- Despliegue de Metasploitable2 para practica con Metasploit

9.2 Herramientas de Pentesting

Se planea instalar un conjunto de herramientas profesionales de pentesting en el servidor empresa:

- Kali Linux como contenedor Docker con herramientas preinstaladas
- Metasploit Framework para explotacion de vulnerabilidades
- Nmap y Nessus para escaneo y enumeracion
- Burp Suite para pentesting de aplicaciones web
- Wireshark para analisis de trafico de red

9.3 Gestion de Vulnerabilidades

Implementacion de una plataforma de gestion de vulnerabilidades y reportes:

- Despliegue de DefectDojo para gestion de hallazgos
- Integracion con herramientas de escaneo automatico
- Generacion de informes profesionales de pentesting

9.4 Mejoras de Seguridad

Ampliaciones planificadas para reforzar la seguridad de la infraestructura:

- Implementacion de Wazuh como SIEM para deteccion de intrusiones
- Certificados SSL/TLS con Let's Encrypt para los servicios web
- Autenticacion de doble factor (2FA) en Portainer y Grafana

- Logs centralizados con Graylog o ELK Stack

9.5 Documentacion de Pruebas

Una vez completada la infraestructura se realizaran y documentaran las siguientes pruebas:

- Prueba de penetracion completa sobre la red DMZ
- Ataques controlados sobre los contenedores vulnerables del laboratorio
- Documentacion de vulnerabilidades encontradas y su explotacion
- Redaccion de informes de pentesting profesionales con recomendaciones