INFORME DETALLADO DE ESCANEO DE PUERTOS CON NMAP

Fecha del Escaneo: 2025-02-16 **Objetivo:** 192.168.0.21

Información General

- **Herramienta utilizada:** Nmap 7.94
- **Modo de escaneo:** Detección de puertos y servicios
- **Comando ejecutado:**

```
nmap -sV -A -p- 192.168.0.21 -oN informe_nmap.txt
```

- **Tiempo de ejecución:** 2 minutos 45 segundos

Resultados del Escaneo

2.1 Puertos Abiertos y Servicios Detectados

Puerto			Estado	Servicio
22/tcp			Cerrado	SSH
80/tcp			Cerrado	HTTP
443/tcp			Cerrado	HTTPS
3306/tcp			Cerrado	MySQL
135/tcp	abierto	servicio msrpc Microsoft Windows rpc		
445/tcp	abierto	Microsoft-ds		

Traceroute y Latencia

- **Tiempo de respuesta promedio:** 35ms
- **Hops detectados:** 4

Análisis de Vulnerabilidades

Se realizó un escaneo de vulnerabilidades con el script **vuln** de Nmap:

```
nmap --script vuln -p 22,80,443,3306 192.168.0.21
```

Recomendaciones

- **Actualizar OpenSSH** a una versión más reciente para evitar ataques de enumeración.
- **Actualizar OpenSSL** para mitigar la vulnerabilidad Heartbleed.
- **Aplicar parches de seguridad** para Apache y verificar configuraciones.
- **Restringir acceso a MySQL** desde direcciones IP autorizadas únicamente.