Informe de Escaneo de Red con Nmap

# 1. Información General

Fecha del escaneo: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nombre del auditor: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Rango de IPs escaneadas: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 2. Resultados del Escaneo

Resumen de hosts escaneados:

|  |  |  |  |
| --- | --- | --- | --- |
| Dirección IP | Puertos Abiertos | Servicios Detectados | Sistema Operativo (si aplica) |
| 192.168.1.X | 80, 443 | HTTP, HTTPS | Windows 10 |
| 192.168.1.X | 80, 443 | HTTP, HTTPS | Windows 10 |
| 192.168.1.X | 80, 443 | HTTP, HTTPS | Windows 10 |
| 192.168.1.X | 80, 443 | HTTP, HTTPS | Windows 10 |
| 192.168.1.X | 80, 443 | HTTP, HTTPS | Windows 10 |

# 3. Análisis y Observaciones

Describa los hallazgos relevantes del escaneo, como servicios inseguros, configuraciones sospechosas o vulnerabilidades detectadas.

# 4. Recomendaciones

Incluya sugerencias para mitigar los riesgos detectados, como cerrar puertos innecesarios, actualizar servicios o implementar firewalls.

# 5. Evidencias (opcional)

Adjunte capturas de pantalla o archivos de salida del escaneo si es necesario.