**Reporte de escaneo a la ip: 192.168.238.130**

Principalmente se realize un escaneo para verficar servicios y versions de la maquina victima, y estos fueron los resultados colectados:

**A screenshot of a computer

Description automatically generated**

Luego se procedio a realizar un scaneo mas a fondo para descubri que Sistema operative tenia la maquina victima y estos fueron los datos obtenidos:

**A screenshot of a computer

Description automatically generated**

Para finalizar se realizo un analisis de vulnerabilidades a la maquina victima, y debido a la cantidad tan grande de vulnearabilidades que esta tiene se realize un resumen de las mas importantes:

**Análisis de Vulnerabilidades**

El análisis de vulnerabilidades realizado por Nmap ha identificado varias vulnerabilidades críticas en los puertos 80, 443, 445, y 3389. A continuación, se detalla el impacto y las medidas recomendadas para mitigar cada una de ellas:

1. **Puertos 80 y 443 (HTTP y HTTPS) - Vulnerabilidades en Servidores Web:**
   * **Impacto:** Los servidores web con versiones antiguas o mal configuradas pueden ser susceptibles a ataques como inyecciones SQL, cross-site scripting (XSS), y ejecución remota de código (RCE). Si no se aplica una adecuada política de seguridad, un atacante podría tomar el control del servidor o exfiltrar información sensible.
   * **Recomendaciones:**
     + Actualizar el servidor web a la última versión disponible.
     + Implementar políticas de seguridad como Content Security Policy (CSP) y asegurar que los encabezados HTTP estén correctamente configurados.
     + Utilizar herramientas como ModSecurity para la detección y prevención de intrusiones (IDS/IPS).
     + Realizar auditorías periódicas de seguridad para identificar y mitigar vulnerabilidades.
2. **Puerto 445 (SMB - Server Message Block):**
   * **Impacto:** El puerto 445 es comúnmente explotado por ataques como el ransomware (e.g., WannaCry) que aprovechan vulnerabilidades en SMBv1. Estas vulnerabilidades permiten a un atacante ejecutar código arbitrario en el sistema afectado, comprometiendo completamente la red.
   * **Recomendaciones:**
     + Deshabilitar SMBv1 y asegurar que solo SMBv2 o SMBv3 estén en uso.
     + Aplicar las actualizaciones de seguridad más recientes para el protocolo SMB.
     + Restringir el acceso al puerto 445 desde fuera de la red local mediante firewalls y reglas de filtrado.
     + Monitorear activamente el tráfico SMB en busca de actividades sospechosas.
3. **Puerto 3389 (RDP - Remote Desktop Protocol):**
   * **Impacto:** El puerto 3389 es un objetivo común para ataques de fuerza bruta y vulnerabilidades RCE en servicios de RDP mal configurados. Un atacante que explote una vulnerabilidad en RDP puede obtener acceso remoto al escritorio de un usuario o servidor, comprometiendo completamente el sistema.
   * **Recomendaciones:**
     + Asegurarse de que el acceso RDP esté restringido únicamente a usuarios autorizados mediante el uso de listas blancas de IPs y/o VPNs.
     + Habilitar la autenticación de nivel de red (NLA) para RDP.
     + Deshabilitar el RDP si no es estrictamente necesario.
     + Mantener RDP actualizado con los últimos parches de seguridad.
     + Implementar políticas de bloqueo de cuentas después de múltiples intentos fallidos de inicio de sesión para mitigar ataques de fuerza bruta.

Estas recomendaciones ayudarán a mitigar los riesgos asociados con las vulnerabilidades detectadas y protegerán tu infraestructura de posibles ataques.