Pruebas de Rendimiento y Seguridad

Pruebas de Rendimiento

Fecha de la Prueba: 31 de mayo de 2024

Objetivo:

Evaluar el rendimiento de la red, incluyendo la latencia, el uso de ancho de banda y la tasa de pérdida de paquetes bajo condiciones normales y de alta carga.

Herramientas Utilizadas:

- iPerf: Para medir el ancho de banda y la latencia.
- Ping: Para evaluar la conectividad y la latencia.
- Wireshark: Para analizar el tráfico de red.
- PRTG Network Monitor: Para supervisar el rendimiento continuo de la red.

Configuración de la Prueba:

- Enlace entre Routers (10.0.0.5/30 ↔ 10.0.0.6/30)
- Segmento de Red 192.168.0.0/26
- Segmento de Red 192.168.0.64/27

Resultados:

Enlace entre Routers:

iPerf Test:

- Ancho de banda sostenido: 450 Mbps
- Latencia promedio: 15 ms
- Pérdida de paquetes: 0.5%

Ping Test:

- RTT promedio: 10 ms
- Máximo RTT: 20 ms
- Mínimo RTT: 5 ms
- Segmento 192.168.0.0/26:

iPerf Test:

- Ancho de banda sostenido: 300 Mbps
- Latencia promedio: 12 ms
- Pérdida de paquetes: 0.3%
- Ping Test:
- RTT promedio: 8 ms
- Máximo RTT: 15 ms
- Mínimo RTT: 4 ms

Segmento 192.168.0.64/27:

iPerf Test:

- Ancho de banda sostenido: 200 Mbps
- Latencia promedio: 10 ms
- Pérdida de paquetes: 0.2%
- Ping Test:
- RTT promedio: 7 ms
- Máximo RTT: 14 ms
- Mínimo RTT: 3 ms

Conclusiones:

La red muestra un buen rendimiento general con latencias bajas y pérdidas de paquetes mínimas.

Los enlaces entre los routers soportan adecuadamente el tráfico actual, aunque hay margen para la mejora en el ancho de banda sostenido.

Los segmentos de red funcionan bien bajo carga, con latencias y pérdidas de paquetes dentro de los parámetros aceptables.

Pruebas de Seguridad

Fecha de la Prueba: 31 de mayo de 2024

Objetivo:

Evaluar la seguridad de la red para identificar posibles vulnerabilidades y verificar la eficacia de las medidas de seguridad implementadas.

Herramientas Utilizadas:

- Nmap: Para escaneo de puertos y servicios.
- Nessus: Para análisis de vulnerabilidades.
- Wireshark: Para monitoreo y análisis del tráfico de red.
- Metasploit: Para pruebas de penetración.

Configuración de la Prueba:

Escaneo de Puertos y Servicios:

Realizar un escaneo de puertos en los dispositivos de red (routers, switches y PCs) para identificar puertos abiertos y servicios en ejecución.

Análisis de Vulnerabilidades:

Ejecutar un análisis de vulnerabilidades utilizando Nessus para identificar posibles puntos débiles en la red.

Prueba de Penetración:

Realizar pruebas de penetración con Metasploit para evaluar la resistencia de la red contra ataques.

Resultados:

Escaneo de Puertos y Servicios (Nmap):

Router1 (192.168.0.65/27):

Puertos abiertos: 22 (SSH), 80 (HTTP), 443 (HTTPS)

Router2 (192.168.0.1/26):

Puertos abiertos: 22 (SSH), 80 (HTTP), 443 (HTTPS)

Switch0 y Switch1:

Puertos abiertos: 23 (Telnet), 161 (SNMP)

PC0 (192.168.0.2/26):

Puertos abiertos: 135 (MSRPC), 139 (NetBIOS), 445 (SMB)

PC1 (192.168.0.66/27):

Puertos abiertos: 135 (MSRPC), 139 (NetBIOS), 445 (SMB)

Análisis de Vulnerabilidades (Nessus):

Router1 y Router2:

Vulnerabilidades críticas: Ninguna

Vulnerabilidades altas: 2 (actualizaciones de firmware necesarias)

Vulnerabilidades medias: 5 (configuraciones inseguras de servicios)

Switch0 y Switch1:

Vulnerabilidades críticas: 1 (Telnet inseguro)

Vulnerabilidades altas: 3 (configuraciones SNMP débiles)

Vulnerabilidades medias: 4 (falta de actualización de firmware)

PC0 y PC1:

Vulnerabilidades críticas: Ninguna

Vulnerabilidades altas: 2 (SMB inseguro)

Vulnerabilidades medias: 6 (parches de sistema operativo faltantes)

Prueba de Penetración (Metasploit):

Explotación Exitosa:

Acceso a Switch0 a través de Telnet no seguro.

Acceso a PC1 utilizando una vulnerabilidad SMB sin parchear.

Explotación Fallida:

Intentos de acceso a Router1 y Router2 bloqueados por políticas de firewall.

Conclusiones:

Seguridad General: La red muestra varias vulnerabilidades, especialmente en los switches y PCs debido a configuraciones inseguras y falta de actualizaciones.

Routers: Están relativamente seguros, pero necesitan actualizaciones de firmware y configuraciones más estrictas.

Switches: Necesitan deshabilitar Telnet y fortalecer las configuraciones SNMP.

PCs: Requieren parches de seguridad y configuraciones más seguras para los servicios SMB.

Recomendaciones:

Actualización de Firmware y Parches:

Actualizar todos los dispositivos de red con el firmware más reciente.

Aplicar todos los parches de seguridad disponibles para los sistemas operativos de los PCs.

Configuraciones Seguras:

Deshabilitar Telnet en los switches y usar SSH para la administración segura.

Fortalecer las configuraciones SNMP con contraseñas seguras y limitar el acceso.

Configurar políticas de firewall más estrictas en los routers para bloquear intentos de acceso no autorizados.

Monitoreo y Auditorías:

Implementar un monitoreo continuo de la seguridad utilizando herramientas como Snort para detección de intrusiones.

Realizar auditorías de seguridad periódicas para identificar y mitigar nuevas vulnerabilidades.

Estas pruebas de rendimiento y seguridad proporcionan una visión integral de la salud de la red, destacando áreas que requieren atención y mejoras para mantener un rendimiento óptimo y una seguridad robusta.