Ejercicios: Herramientas de Análisis Local

Taller Gestión de Redes
WALC 2009: 21-25 Septiembre 2009
Bogotá, Colombia

1.) LSOF y NETSTAT

Vea que servicios están corriendo en tu maquina. Puedes usar la presentación como referencia:

https://nsrc.org/trac/netmanage/attachment/wiki/Walc2009Presentaciones/analisis_desempeno_servidor.pdf

O, utiliza "man lsof", "man netstat", "lsof -h" y "netstat -h" para ver las opciones disponibles (hay muchos!). Debería hacer estés ejercicios como el usuario "*root*"

* Usando lsof, que servicios de Ipv4 están escuchando (LISTENing) en tu maquina?

* Usando netstat, que servicios de Ipv4 y Ipv6 están escuchando (LISTENing) en tu maquina?

2.) TCPDUMP y WIRESHARK

Para usar tcpdump tienes que ser root. Para usar wireshark tienes que abrir un terminal y usar sudo como un usuario normal (ej:, como usuario "walc"):

* En un terminal de root usa tcpdump como esto:

  ```
  # tcpdump -i lo -A -s1500 -w /tmp/tcpdump.log
  ```

  Ahora, genera algo de trafico en tu interfaz "lo" en otro terminal.
  Por ejemplo:

  ```
  $ ping localhost
  $ ssh localhost
  ```

  etc. Después, apreta CTRL-C para terminar la sesión de tcpdump

* En otro terminal, como usuario normal (ej: como "walc") abre wireshark asi:

  ```
  $ sudo wireshark -r /tmp/tcpdump.log
  ```

  Ahora puedes jugar con el interfaz de wireshark para empezar de entender como se lo funciona. Puedes resolver como seguir paquetes por protocolo? Sesión?

3.) USANDO IPERF

Usa "man iperf" o "iperf -h" por ayuda.

* Pide a tu vecino que corren "iperf -s". Conectate a la maquina de tu vecino usando "iperf -c ipVecino". Como es el rendimiento entre sus maquinas?

* Prueba TCP usando varias tamaños de ventanas (opcion “-2”).

* Verifica TCP MSS (-m). Como se afecta el rendimiento? Que es el “Path MTU discovery?”

* Prueba con dos sesiones en paralelo (-P) y comparar los totales. Hay una diferencia? Porque?

* Prueba con otros tamaños de paquetes y con el TCP_NODELAY (-N) opción.

3.) MAS PARA HACER

Si, ya, terminaste con todo puede leer la presentación y jugar con:

* nmap
* vmstat
* top
* ntop