TP 1 - Herramientas de Diagnóstico de Redes

Fecha de Entrega: Chivilcoy: 28/08/2023. Luján: 30/08/23

Objetivo: Conocer el funcionamiento y familiarizarse con las herramientas que permiten explorar, diagnosticar problemas y medir diferentes aspectos de una red. Categorías ISO: **F**C**AP**S.

Tanto en este práctico como en los sucesivos, es sumamente conveniente que realicen una transcripción de lo escrito y obtenido por pantalla. Para ello, antes de iniciar la práctica, ejecute el comando `script guardado_de_salida_fecha.txt` . Al finalizar los ejercicios, escriba el comando `exit` para cerrar y guardar el archivo. Toda la documentación de los comandos que se utilizarán se puede obtener con `man comando` .

Bibliografía

- OPPENHEIMER, P., 2011, *Top-Down Network Design (3d ed).* CISCO Press.
  - Capítulo 2. Sección “Network Performance” (pp. 32-44)
  - Capítulo 3. Sección “Checking the Health of the Existing Internetwork” (pp. 71-81)

Experiencia de laboratorio

ping (RTT)

A pesar de su simpleza `ping` continúa siendo una herramienta realmente útil para obtener una estimación del tiempo de ida y vuelta (Round-Trip Time) entre dos hosts.

1. Destine cinco minutos a elegir siete destinos contra los cuales realizar una medición de RTT. Deberán estar ubicados: uno en su misma provincia, el segundo en otra provincia, y los restantes en cada uno de los cinco continentes. Verifique mediante algún método (ej: geoip) que cada host remoto se encuentra en el lugar geográfico correspondiente. Configure `ping` para enviar Echo Request cada 0.5 segundos hasta alcanzar 600 mensajes. Refiérase al manual de la herramienta (`man ping`) para determinar qué parámetros permiten establecer tal configuración.

   Presente los resultados finales contra cada host en una tabla con la siguiente estructura:

		Latencia			Porcentaje
Host Destino	Ubicación	Mínima	Promedio	Máxima	Desvío	de Pérdida

2. ¿Qué observa a partir de las mediciones reflejadas en la tabla? ¿A qué podría deberse?

traceroute

El comando `traceroute` aprovecha ciertas particularidades del protocolo IP para intentar obtener y mostrar en pantalla el camino que toma un paquete al ir de un host a otro. Además, si recibe respuesta, muestra el RTT percibido hasta cada uno de los dispositivos que forman el camino.

1. Instale la herramienta y explique como funciona. Luego de efectuar una prueba contra un host remoto ¿qué significan las lineas `*.*.*.*` en la salida del programa?
2. Realice `traceroute` a los hosts definidos en el ejercicio de `ping` anterior. Adicione a la tabla previa una columna con la cantidad de dispositivos intermedios.
3. Una vez que finaliza el descubrimiento de la ruta con traceroute, ¿Se puede afirmar que todos los paquetes IP (de la prueba que ejecutó esa instancia del programa) siguieron exactamente esa misma ruta? Justifique su respuesta.

nmap (exploración de la red)

Herramienta para escaneo de puertos y exploración de redes. Las referencias básicas son el manual (`man nmap`) y el sitio oficial http://nmap.org.

1. Instale `nmap` en su equipo. Ejecute un escaneo básico contra el equipo indicado por el docente y a su propio equipo.

   ```
   $ nmap -Pn 190.104.80.3
   $ nmap localhost
   ```

   ¿Qué información brinda la salida del comando? ¿Qué rol tiene ese host en la organización? ¿En qué medida esta información puede ser útil o peligrosa para una organización?

2. Realice un escaneo utilizando `nmap` sobre la red de las aulas, identifique las funciones de los hosts a partir de la información que pueda extraer utilizando dicha aplicación.

iperf (throughput)

Constituye una herramienta que permite medir el *throughput* y la calidad de un enlace. Para ello, emplea un esquema cliente-servidor. *Este punto lo puede resolver utilizando máquinas virtuales o bien si así lo dispone utilizando dos equipos físicos. También puede consultar el listado de servidores iperf públicos*

1. Iniciar el servidor correspondiente para que reciba peticiones en un puerto diferente al definido por defecto. Verifique si la operación fue exitosa empleando el comando `netstat` (paquete net-tools) o bien mediante el comando `ss -tnlp` . Adjuntar salida del comando.
2. Verificar el *throughput* existente con otro equipo perteneciente a la red del laboratorio bajo los protocolos TCP y UDP durante 60 segundos en intervalos de 5 segundos.

ab (test de estrés para servidores web)

Herramienta para realizar *benchmarking* de Servidores Web. Se encuentra diseñada para proporcionar una aproximación del rendimiento actual del servidor, exhibiendo específicamente cuántas peticiones por segundo el mismo es capaz de servir.

1. Instale la herramienta `ab` (paquete `apache2-utils` en Debian).
2. Realice una prueba contra el servidor web https://eula-gtec.unlu.edu.ar/ efectuando 1000 peticiones con una concurrencia de 10 peticiones simultáneas. **Nota:** no omita la barra final de la dirección web.
3. ¿Qué información proporciona la herramienta? Grafique la prueba realizada (**Ayuda**: Opciones `-e` , `-g`)
4. ¿Qué implica la utilización del parámetro `-i` ? ¿Qué diferencia encuentra con la prueba de la consigna previa?

Trabajo práctico

ping (RTT)

1. Instale y configure la herramienta SmokePing. Mida durante al menos dos horas contra 3 hosts localizados en distintos continentes (puede emplear aquellos de la consigna previa). Adjunte los gráficos correspondientes a las mediciones realizadas y comente los

comportamientos que puede observar a partir de ellos.
Encontrará una breve guía de configuración de la herramienta adjunta a esta práctica.

2. ¿Qué comportamiento se observa? ¿Qué implicaría un incremento/disminución de la latencia a partir de un patrón establecido? ¿Qué otras utilidades ofrece esta herramienta?
3. ¿De qué manera afecta la latencia a las aplicaciones? Describa y brinde ejemplos.

traceroute

1. Verifique la ruta que podría llegar a seguir un paquete IP hacia el host `8.8.8.8` (servidor DNS público de Google). Ejecute la misma consulta varias veces y en momentos distintos ¿Qué conclusión puede obtener?
2. En qué situaciones puede llegar a ser útil esta herramienta. Ejemplifique.
3. En una red externa a la Universidad, realice `traceroute` al sitio web `www.unlu.edu.ar` y otro a `www.ut.ee` . Indique el ISP que provee el servicio de conectividad a Internet en ese momento. Adjunte la salida del traceroute. En clase, compare su salida contra el de sus compañeros. ¿Hay dispositivos (hosts o direcciones IP) en común entre las salidas de sus pares? ¿Cuáles son?

nmap (exploración de la red)

1. Lea el manual de la herramienta y ejecute el ejercicio 1 de la experiencia de laboratorio contra `localhost` . Comente que información adicional visualiza respecto al ejercicio anterior. Compárelo con la ejecución del ejemplo 1 al dominio de la UNLu, y comente brevemente por qué una mala configuración puede representar un riesgo de seguridad.
2. Una de las ventajas de nmap es que permite, mediante comodines o con formato CIDR, hacer un escaneo completo de un segmento de red para descubrir dispositivos presentes en la misma. Busque en el manual la sección “TARGET SPECIFICATION” (o bien en español: ESPECIFICACIÓN DE OBJETIVOS) y deduzca como puede encontrar todos los dispositivos conectados a su red. Puede ver su dirección IP actual mediante el comando `ip addr show` .
3. Investigue que opción permite hacer escaneo de puertos UDP y luego utilícela contra un host particular. ¿Por qué podría resultar útil realizar un análisis de ésta característica, si la mayoría de los servicios de red utilizan TCP?
4. Instale en un equipo de su hogar la aplicación `nmap` y realice un escaneo a toda la red de su hogar. ¿Que ha logrado descubrir? ¿Existen otros host aparte de su equipo? ¿Qué puertos poseen en escucha? ¿se corresponden con los servicios que usted esperaba?

iperf (throughput)

1. En el caso de TCP: Realice mediciones empleando diversos tamaños de ventana. Considerando valores: 1kb, 2kb, 16kb, 128kb, 320kb, 10mb Confeccione una gráfica que represente el *throughput* respecto del tamaño de ventana efectivamente asignado por el programa.
2. ¿Qué permite establecer la opción `-M` ? ¿Cómo afecta esto al *throughput*? Investigue la técnica “Path MTU discovery”.
3. ¿Qué efecto presenta la opción `-N` ? ¿Qué tipo de aplicaciones pueden requerir tal utilidad?

iptraf (estadísticas de uso de la red)

iptraf es una herramienta para monitorizar redes IP. Intercepta los paquetes que cursan la red y presenta varias estadísticas acerca del tráfico actual en ella.

1. Inicie la utilidad mediante el comando `iptraf-ng` (como usuario `root`).

2. Consulte las opciones “IP Traffic Monitor”, “Detailed Interface Statistics” y visite el sitio web de la UNLu y otros sitios. ¿Qué información proporciona cada opción?
3. Configure la herramienta para que genere un archivo log de la información recuperada. Vuelva a consultar las opciones de la consigna anterior. ¿En que ruta por defecto se almacena tal información? ¿Para qué podría utilizarse?

ntop (estadísticas de uso de la red)

Herramienta para el monitoreo y análisis de tráfico en la red. Provee una interfaz web para los reportes muy completa e intuitiva.

1. Instalar `ntop` en su distribución. El servicio levanta automaticamente, si no lo hace Iniciar ntop en su forma básica: como root o con sudo:
   `ntop -i <interfaz de red>`
2. Luego ingrese vía web browser a http://localhost:3000.
   Debería estar visualizando la interfaz de ntop.
3. Revise los menus “Summary”, “All protocols” e “IP”. Comente muy brevemente las opciones que le resulten mas útiles o interesantes. Si visualiza poca información, navegue por un par de sitios externos y vuelva a recargar la pagina de Ntop (F5).
4. ¿Porque cree que se necesita ejecutar con permisos de root?
5. Para los siguientes requerimientos de información, aclare que opción de ntop es la mejor, y comente brevemente que información ofrece.
   - Si necesita ver con ntop un resumen del trafico de los protocolos de la Capa de Aplicación del stack TCP/IP, ¿a que opción debería dirigirse?
   - Si el administrador necesita revisar la actividad de la red por periodo de tiempo, cual listado de ntop ofrece una mejor visualización al respecto.

Herramientas gráficas

1. Investigue qué herramientas gráficas existen para monitorear redes y centros de datos. Seleccione una y comente sus funcionalidades.

Guía de lectura

De la siguiente lista de herramientas, lea la sinopsis, la descripción y los ejemplos de las páginas de manual correspondiente a cada una de ellas (`man herramienta` en la terminal o bien en línea):

> ps, htop, netstat, ip link, ip addr, ip neigh, ss, mii-tool, ping, arping, traceroute, netperf, iperf, iptraf (iptraf-ng), tcpdump, tshark, rfkill, inxi, wireshark, speedtest (speedtest-cli), vnc (tigervnc), ssh, dig, nslookup, hping (hping3), iotop, nmcli, curl, wget, smokeping, apachebench (ab), nmap, netcat (nc), telnet, iw, resolvectl, dsniff, ethtool, nethogs

Categorice las mismas según su objetivo principal:

- Configuración y/o determinación de estado
- Prueba de conectividad
- Determinación y prueba de caminos
- Pruebas de throughput
- Captura de tráfico/paquetes
- Descubrimiento de dispositivos y servicios

- Determinación de la performance
- Pruebas de protocolos de capa de enlace y/o red
- Pruebas de protocolos de capa de aplicación
- Pruebas de seguridad
- Acceso remoto