

Taller Practico Principios de Redes :**1.0 Usando Windows****1.1 Comandos básicos**

- **ping destino** : Nos informa del estado de un host. Es necesario permitir paquetes ICMP para su funcionamiento.
- **ping destino -t** : Se hace ping hasta que que pulsemos Ctrl+C para detener los envíos.
- **tracert destino** : Indica la ruta por la que pasa nuestra petición hasta llegar al host destino.
- **tracert -d destino** : No resuelve los nombres del dominio.
- **tracert -h (valor)** : Establece un numero máximo de saltos.
- **ipconfig** : Proporciona información sobre TCP/IP, adaptadores, muestra información general sobre la red.
- **ipconfig /all** : Ofrece información detallada sobre todas las tarjetas de red y conexiones activas.
- **ipconfig /renew** : Renueva petición a un servidor DHCP
- **ipconfig /release** : Libera la Ip asignada por DHCP
- **net Start** : Inicia un servicio de Windows
- **net Stop** : Detiene un servicio de Windows
- **netstat** : Muestra todas las conexiones activas en el equipo.
- **netstat -a** : Nos muestra todas las conexiones y puertos.
- **netstat -e** : Muestra las estadísticas Ethernet
- **netstat -n** : Muestra direcciones y puertos en forma de numero.
- **netstat -o** : Muestra que programa esta asociado a la conexion activa
- **arp** : Muestra y modifica datos de la tabla de traduccion de direcciones IP a direcciones MAC (tabla ARP)
- **arp -a (ó -n -g)** : Muestra la tabla ARP para cada uno de los interfaces
- **route** : Muestra y modifica la información sobre las rutas IP del equipo.
- **hostname** : Muestra el nombre de la computadora

HOSTS (sin extensión alguna), es un archivo utilizado por Windows para asociar nombres de dominio con direcciones IP. Si este archivo existe en c:\windows\ (Windows 95, 98 y Me), o en \system32\drivers\etc\ (Windows NT, 2000, XP, Vista y 7), el sistema lo examina antes de hacer una consulta a un servidor DNS. Tenga en cuenta que no necesariamente debe existir en todos los sistemas.

Algunos malwares modifican HOSTS para que el usuario no pueda ingresar a algunos sitios (generalmente para impedir la actualización de antivirus u otro software de seguridad), o para que sea redirigido a sitios falsos.

Por ejemplo, cualquiera de las siguientes líneas en el archivo HOSTS, impediría que el usuario ingresara al sitio "**www.ejemplo.com**", cuya verdadera IP (en este caso ficticia) pudiera ser "**254.56.78.12**", si teclea solo "**http://www.ejemplo.com**" en la barra de navegación del navegador:

```
127.0.0.1                www.ejemplo.com
0.0.0.0                  www.ejemplo.com
```

NOTA: Las direcciones **0.0.0.0** (ruteo por defecto) y **127.0.0.0** (loopback o retorno

de lazo) tienen un especial significado, y generalmente apuntan a la propia máquina (localhost).

Si en cambio alguien coloca lo siguiente en el archivo HOSTS:

```
230.127.34.9 www.ejemplo.com
```

Entonces el usuario sería redirigido a otra máquina (230.127.34.9) en lugar de la verdadera a la que corresponde **www.ejemplo.com** (254.56.78.12).

Algunas utilidades (Spybot Search and Destroy por ejemplo), agregan al HOSTS direcciones de conocidos sitios que descargan adwares o spywares (comúnmente denominados parásitos), para que estos nunca sean accedidos. Un ejemplo:

```
127.0.0.1 redtauros.com
127.0.0.1 equipo1.com
127.0.0.1 lahuaca.com
```

Normalmente solo el siguiente valor está definido por defecto:

```
127.0.0.1 localhost
```

Existen utilidades (como ZoneAlarm por ejemplo), que agregan una protección contra la modificación no autorizada del archivo HOSTS.

Restaurar archivo HOSTS

1. Utilizando el Explorador de Windows, busque el archivo HOSTS (sin extensión), en alguna de las siguientes carpetas (según el sistema operativo utilizado):

```
c:\windows\
c:\windows\system32\drivers\etc\
c:\winnt\system32\drivers\etc\
```

2. Si aparece, haga doble clic sobre dicho archivo (HOSTS). Seleccione "Seleccionar el programa de una lista", "Aceptar", y luego seleccione NOTEPAD (Bloc de notas). NO MARQUE "Utilizar siempre el programa seleccionado para abrir este tipo de archivos".

3. Borre todas las líneas que comiencen con un número, salvo las siguientes:

```
127.0.0.1 localhost
```

4. Acepte guardar los cambios al salir del bloc de notas.

5. Si utiliza algún programa anti-spyware o anti-adware que modifique el archivo HOSTS para protegerlo de ciertos parásitos, vuelva a ejecutar ese programa para actualizar el archivo HOSTS con dicha información.

1.2 Taller Practico

1. Identificar y conocer las instrucciones.
2. Identificar la IP del equipo (Nivel del modelo OSI, clase, mascara, dirección IP - Que instrucción uso y que respuesta dio el sistema).
3. Identificar la Dirección MAC del equipo (Nivel del modelo OSI - Que instrucción uso y que respuesta dio el sistema).
4. Identificar el Gateway o Pasarela de la red. (Cual es?)

5. Realizar ping de un equipo a otro (Que instrucción uso y que respuesta dio el sistema).
6. Crear dos redes distintas. (Cuales se crearon, que red son y que mascara tienen).
7. Probar si da Ping (Que instrucciones uso, que respuestas dio el sistema y de una breve explicación de lo que paso).
8. Identificar la ARP del equipo (Que instrucción uso y que respuesta dio el sistema).
9. Identificar la IP de Google (Que instrucción uso y que respuesta dio el sistema).
10. Realizar un ping al localhost e identificar el nombre (Que instrucción uso?).
11. Adicionar en el archivo hosts esta linea: 127.0.0.1 google.com (Que pasa cuando entro en el navegador a google.com?)
12. Adicionar en el archivo hosts esta linea: 192.168.0.102 equipo1.utap.com (Que pasa cuando entro en el navegador a equipo1.utap.com?)

Taller completo entregado a mas tardar el día del parcial : + 0.2 en la nota del Parcial.