



UF 1. Implantación de arquitecturas web

ACTIVIDAD 1 COMANDOS

AUTOR: JAVIER PÉREZ
VIVAR

ENERO DE 2021

Contenido

Enunciado.....	3
Desarrollo actividad	4
1.- ¿Cómo sabemos si tenemos conexión a internet? Pista: ifconfig, ping.....	4
1.1.- Comando IPCONFIG (En Linux se utiliza IFCONFIG):	4
1.2.- Comando PING (En Linux es igual)	5
2.- ¿Cómo sabemos si nuestro servidor es accesible desde Internet? Pista: ufw, netstat	5
2.1.- UFW.....	6
2.2.- Netstat.....	6
3.- ¿Cómo sabemos a quién pertenece una dirección web (URL)? Pista: dig, nslookup	7
3.1.- DIG.....	7
3.2.- NSLOOKUP.....	8
4.- ¿Cómo probamos que podemos acceder a un servidor? Pista: curl, wget.....	10
4.1.- WGET.....	10
4.2.- CURL	10
5.- ¿Qué otros comandos te han hecho falta?	12

Enunciado

Requerimiento 1

La administración de un servidor web y/o un servidor de aplicaciones requiere unos conocimientos básicos de comandos de consola que permite visualizar qué está pasando en nuestro servidor. Se pide practicar y crear una guía de uso para las siguientes problemáticas que nos podemos encontrar:

¿Cómo sabemos si tenemos conexión a internet? Pista: ifconfig, ping

¿Cómo sabemos si nuestro servidor es accesible desde Internet? Pista: ufw, netstat

¿Cómo sabemos a quién pertenece una dirección web (URL)? Pista: dig, nslookup

¿Cómo probamos que podemos acceder a un servidor? Pista: curl, wget

¿Qué otros comandos te han hecho falta?

Valoración: 10 puntos sobre 10

Consideraciones

Para toda la actividad se valorará el orden y la claridad de la documentación, así como la facilidad de uso.

Para la entrega, es necesaria la creación y subida a la plataforma de un pequeño documento formal sobre la actividad (portada, explicación, etc.) y una guía "how-to" que describa y permita resolver las preguntas planteadas en la actividad*.

Nótese que más adelante se pedirá que se realicen tareas con un repositorio GIT que contenga la documentación de esta actividad.

* Se recomienda crear un repositorio GitHub para almacenar la guía "how-to" en formato texto y/o Markdown.

Se considerará a la hora de evaluar la facilidad de uso de dicha guía que se explique de manera clara y sencilla:

- Qué hace el comando
- Cómo se usa
- Por qué responde a la pregunta
- Cómo se interpreta la salida

Desarrollo actividad

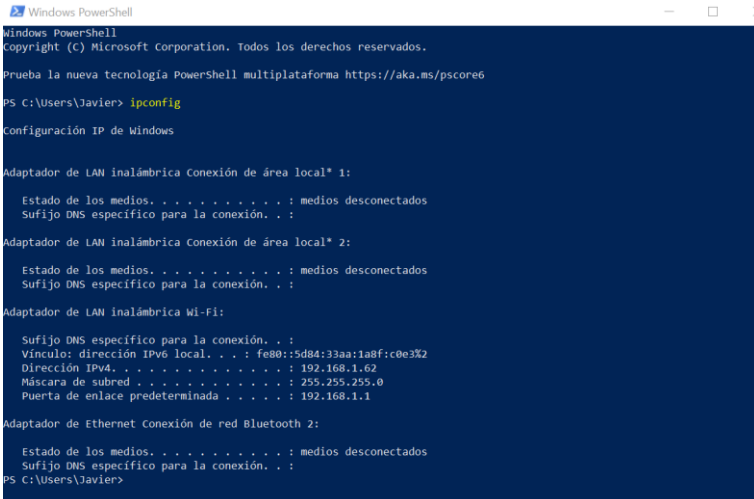
En la presente guía, vamos a conocer a como obtener a través de la herramienta “PowerShell” del SO Windows, diferente información que nos puede ser útil a la hora de configurar y administrador nuestro equipo.

1.- ¿Cómo sabemos si tenemos conexión a internet? Pista: ifconfig, ping

Tenemos varios métodos para conocer el estado de conexión con internet de nuestro equipo, así como nuestra dirección IP, etc. Para ello lo primero que vamos a hacer es abrir la consola de Windows PowerShell (estos comandos también funcionan en CMD).

1.1.- Comando IPCONFIG (En Linux se utiliza IFCONFIG):

- Qué hace el comando
 - Muestra información y todos los datos de la configuración del equipo para el protocolo TCP/IP. Adicionalmente permite liberar y renovar la dirección IP de un adaptador de red y mostrar el contenido de la caché de resolución DNS, así como vaciarla, actualizar y volver a registrar los nombres.
 - Muestra las direcciones IPv6 (Protocolo de Internet versión 4) e IPv6, la máscara de subred y la puerta de enlace predeterminada para todos los adaptadores.
- Cómo se usa
 - En powerShell introducimos el comando sin parámetros
 - PS C:\Users\Javier> ipconfig
- Por qué responde a la pregunta
 - Nos da información sobre los adaptadores tanto de red inalámbrica como Ethernet, mostrándonos si están activos o no y caso afirmativo, las direcciones IP, máscaras de subred, etc.
- Cómo se interpreta la salida
 - La interpretación es muy sencilla, ya que el propio sistema nos indica los adaptadores de red disponibles, si están activos o no y las direcciones IP de nuestra máquina, en el caso de que alguna de las conexiones esté activa.



```

Windows PowerShell
Copyright (c) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\Javier> ipconfig

Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufixo DNS específico para la conexión. . :
    Vínculo: dirección IPv6 local. . . : fe80::5d84:33aa:1a8f:c0e3%2
    Dirección IPv4. . . . . : 192.168.1.62
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . : 192.168.1.1

Adaptador de Ethernet Conexión de red Bluetooth 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . :

PS C:\Users\Javier>
  
```

1.2.- Comando PING (En Linux es igual)

Podemos obtener una información parecida a través de otros comandos tales como PING, que a diferencia del primero el principal objetivo de un ping es ver si un determinado ordenador o servidor es accesible desde otro, es muy útil para diagnosticar problemas en una determinada red.

- Qué hace el comando
 - Es una herramienta comúnmente usada para solucionar problemas de accesibilidad de hosts en una red
 - Ver si una máquina es accesible desde otro
 - Diagnosticar problemas de una red.
- Cómo se usa
 - Aunque tiene diferentes métodos o apellidos que se utilizan para realizar diferentes tareas, la más común es introducir PING + una dirección IP
 - Ej: ping 192.168.1.62
- Por qué responde a la pregunta
 - Porque si una máquina que tiene una dirección determinada se hace ping sobre ella y esta responde, esto quiere decir que está correctamente conectada a una red
- Cómo se interpreta la salida
 - Al hacer ping (o llamadas) a una cierta máquina, esta devuelve cierta información:
 - Tiempo de respuesta: La forma que tenemos de saber que dicha máquina está correctamente conectada es por el tiempo de respuesta, en caso de que no lo esté daría “tiempo de respuesta agotado “
 - Paquetes: En este caso podemos afirmar que la máquina está conectada puesto que tiene un 0% de paquetes perdidos, esto es ha respondido a todos los paquetes enviados.

```
PS C:\Users\Javier> ping 192.168.1.62
Pinging 192.168.1.62 with 32 bytes of data:
Respuesta desde 192.168.1.62: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.62: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.62: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.62: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.62:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
PS C:\Users\Javier>
```

2.- ¿Cómo sabemos si nuestro servidor es accesible desde Internet? Pista: ufw, netstat

2.1.- UFW

En Linux UFW permitir y denegar servicios por puertos, interfaces de red y direcciones IPs. Hay herramientas que nos permiten activar o desactivar el firewall en Windows, el cual lo podemos realizar a través del entorno gráfico o a través de la consola, para ello tecleamos los siguientes comandos.

- `sc config MpsSvc start= auto`
- `net start MpsSvc`
- `netsh advfirewall set allprofiles state off`
- `netsh advfirewall set publicprofile state on`

2.2.- Netstat

- Qué hace el comando
 - De manera básica, al introducir netstat en la consola, nos muestra las conexiones activas que tiene el PC en este momento y el router al que está conectado.
 - Asimismo, a través de diferentes métodos nos muestra, por ejemplo:
 - Comprobar el estado de las redes y servidores a las que se conecta mi máquina
 - Muestra información a tiempo real de todo lo que entra y sale de mi ordenador
 - Podemos, conocer los dispositivos que están conectados a nuestros router, quien está accediendo a tu PC, o para comprobar si la conexión funciona correctamente.
- Cómo se usa
 - En la consola introducimos “netstat” sin parámetros y nos devuelve las conexiones activas que tenemos a tiempo real.
 - Netstat tiene, entre otros los siguientes métodos:
 - **netstat -f**: identificar las conexiones remotas que llegan a nuestro PC, podemos ver los nombres completos de dominio de esas direcciones IP (FQDN).
 - **netstat -n**: identificamos la dirección IP y los puertos que se están utilizando
 - **netstat -e**: Obtenemos estadísticas globales del uso de la red
 - **netstat -a**: muestra todas las conexiones, incluido las inactivas. Así como los puertos de nuestro router que están escuchando (Listening)
 - **netstat -b**: muestra en tiempo real los programas que están conectados a las redes que estemos utilizando, así como el puerto que utilizan.
 - Asimismo, podemos pedirle a netstat Netstat que busque conexiones concretas, como por ejemplo los accesos de Elpais, para ello introducimos `netstat -f | findstr DIRECCION`.
- Por qué responde a la pregunta

- Al mostrarnos todas las conexiones activas sabemos:
 - Que está conectado a la Red
 - El estado de todas las conexiones
 - Los servidores a los que estamos conectados.
 - Las máquinas que están conectadas a nuestros router.
- Cómo se interpreta la salida
 - Nos indica las conexiones activas con los siguientes datos:
 - Protocolo utilizado: TCP
 - Dirección Local: 192.168.1.62: 40679. Siendo:
 1. Los primeros dígitos 192.168.1.62, hasta los dos puntos, la dirección IP
 2. A partir de los dos puntos indica el puerto utilizado.
 - Dirección remota
 - Estado de la conexión
 - Introduciendo los parámetros arriba indicados obteneos información adicional, que utilizaremos según las necesidades de cada momento.

```
PS C:\Users\Javier> netstat
Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    192.168.1.62:49769    a95-100-106-46:https  CLOSE_WAIT
TCP    192.168.1.62:49777    52.155.161.106:https  CLOSE_WAIT
TCP    192.168.1.62:49842    40.101.92.18:https    ESTABLISHED
TCP    192.168.1.62:49843    40.101.92.18:https    ESTABLISHED
TCP    192.168.1.62:49985    93.184.220.29:http    CLOSE_WAIT
TCP    192.168.1.62:49995    52.190.28.19:https    CLOSE_WAIT
TCP    192.168.1.62:50155    192.168.1.61:8009     ESTABLISHED
TCP    192.168.1.62:50211    1drv:https            ESTABLISHED
TCP    192.168.1.62:50214    192.168.1.61:8008     TIME_WAIT
TCP    192.168.1.62:50215    40.67.251.132:https   ESTABLISHED
TCP    192.168.1.62:50234    185.63.145.5:https    CLOSE_WAIT
TCP    192.168.1.62:50235    93.184.220.29:http    CLOSE_WAIT
TCP    192.168.1.62:50289    40.67.251.132:https   ESTABLISHED
TCP    192.168.1.62:50396    a92-123-56-10:https   CLOSE_WAIT
TCP    192.168.1.62:50433    51.138.106.75:https   TIME_WAIT
TCP    192.168.1.62:50437    52.114.158.53:https   TIME_WAIT
TCP    192.168.1.62:50438    52.114.32.24:https    TIME_WAIT
TCP    192.168.1.62:50439    52.114.32.24:https    TIME_WAIT
TCP    192.168.1.62:50442    52.114.32.24:https    ESTABLISHED
TCP    192.168.1.62:50443    52.109.88.174:https   TIME_WAIT
TCP    192.168.1.62:50444    13.107.42.23:https    ESTABLISHED
TCP    192.168.1.62:50445    204.79.197.219:https  ESTABLISHED
TCP    192.168.1.62:50446    a-0001:https          ESTABLISHED
TCP    192.168.1.62:50447    52.114.32.24:https    ESTABLISHED
TCP    192.168.1.62:50448    51.138.106.75:https   ESTABLISHED
TCP    192.168.1.62:50449    1drv:https            ESTABLISHED
TCP    192.168.1.62:50450    52.109.76.124:https   TIME_WAIT
TCP    192.168.1.62:50451    52.109.76.124:https   TIME_WAIT
```

3.- ¿Cómo sabemos a quién pertenece una dirección web (URL)? Pista: dig, nslookup

3.1.- DIG

Es una herramienta que podemos utilizar para consultar servidores.

Se trata de un comando de Unix que permite a los usuarios realizar **consultas a los distintos registros DNS**.

Se puede utilizar en Windows y Linux

Su nombre viene de las siglas Domain Information Groper

Para utilizarlo debemos instalar una herramienta en nuestro PC por lo que vamos a utilizar para esta guía NSLOOKUP, la cual viene preinstalada en Windows y nos da información equivalente.

En el caso de estar interesado en utilizarla la puedes descargar desde el siguiente enlace: [Downloads - ISC](#)

3.2.- NSLOOKUP

- Qué hace el comando
 - NSLOOKUP es una herramienta que viene instalada de manera predeterminada en Windows
 - Nos permite obtener información, probar y solucionar problemas de los servidores DNS que usa una conexión.
- Cómo se usa
 - Al escribir NSLOOKUP en la consola sin especificar ningún parámetro, devolverá el nombre del servidor DNS predeterminado y su dirección IP.
 - Al igual que en los otros comandos en la consola, se introduce el comando, a continuación, las opciones y se hace clic en la tecla Enter, la sintaxis es:


```
nslookup [-opcion] [host] [servidor]
```

 - Donde:
 1. host es la dirección IP o nombre de dominio a consultar
 2. servidor es la IP del servidor en el cual se hará la consulta.
 - Una vez iniciado nslookup, podemos teclear una serie de parámetros y nos devolverá diferente información:
 - **Introducción nombre dominio:** Si se escribe un nombre de dominio (una dirección URL sin el protocolo http://), la consola devolverá la dirección IP de los servidores DNS. Por ejemplo, vamos a introducir "elpais". Como podemos observar abajo, nos devuelva la dirección IP de los servidores y el nombre. El mensaje: "Respuesta no autoritativa" significa que se consulta a un servidor que no posee autoridad directa para el nombre consultado.

```
> elpais.es
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

Respuesta no autoritativa:
Nombre: elpais.es
Addresses: 34.246.117.165
          52.209.191.15
```

- **set type=NS:** especificamos que se nos devuelva los nombres de dominio de los servidores DNS. La forma de utilizarlo es muy sencilla:

1. introducimos **> set type=NS**
2. A continuación, introducimos el dominio, por ejemplo
>elpais.es
3. Obtenemos los nombres de dominio de los servidores DNS

```
> set type=NS
> elpais.es
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254
```

- **Set debug:** Devuelve toda la información disponible sobre ese dominio. La forma de introducir los comandos es similar a la anterior:
 1. **>set debug (Enter)**
 2. **>nombre dominio, ejemplo: elpais.es**

```
> set debug
> elpais.es
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

-----
Got answer:
HEADER:
  opcode = QUERY, id = 12, rcode = NOERROR
  header flags: response, want recursion, recursion avail.
  questions = 1, answers = 4, authority records = 0, additional = 0

QUESTIONS:
  elpais.es, type = NS, class = IN
ANSWERS:
-> elpais.es
  nameserver = ns1.p04.dynect.net
  ttl = 86400 (1 day)
-> elpais.es
  nameserver = ns3.p04.dynect.net
  ttl = 86400 (1 day)
-> elpais.es
  nameserver = ns4.p04.dynect.net
  ttl = 86400 (1 day)
-> elpais.es
  nameserver = ns2.p04.dynect.net
  ttl = 86400 (1 day)

-----
Respuesta no autoritativa:
elpais.es
  nameserver = ns1.p04.dynect.net
  ttl = 86400 (1 day)
```

- **Set type=A:** Con esta opción podemos a través de la dirección IP conocer el dominio, para ello tecleamos:
 1. **>set type=A**
 2. **>Dirección IP, por ejemplo: 8.8.8.8**
 3. Como resultado nos indica el nombre del dominio, en este caso Google

```

> set type=A
> 8.8.8.8
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

-----
Got answer:
HEADER:
  opcode = QUERY, id = 13, rcode = NOERROR
  header flags: response, want recursion, recursion avail.
  questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:
  8.8.8.8.in-addr.arpa, type = PTR, class = IN
ANSWERS:
-> 8.8.8.8.in-addr.arpa
   name = dns.google
   ttl = 55277 (15 hours 21 mins 17 secs)

-----
Nombre: dns.google
Address: 8.8.8.8

```

- Por qué responde a la pregunta
 - Porque, como hemos visto anteriormente si introducimos una dirección IP nos indica el nombre del dominio y viceversa.
- Cómo se interpreta la salida
 - Cuando tecleamos nslookup, el sistema nos indica el servidor predeterminado de la conexión con su dirección IP, como podemos observar abajo.

```

PS C:\Users\Javier> nslookup
Servidor predeterminado: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

```

- A través de nslookup, podemos cambiar el servidor predeterminado, por ejemplo, si escribes: server 8.8.8.8 y presionas Enter, la petición se efectuará a los servidores DNS de Google.

4.- ¿Cómo probamos que podemos acceder a un servidor? Pista: curl, wget

4.1.- WGET

El comando WGET se utiliza en LINUX, para realizar las siguientes tareas:

- Recuperar contenido y archivos de varios servidores web.
- Guardar archivos
- Limitar velocidad de descarga
- Descargar a través de FTP
- Continuar descargas interrumpidas
- Etc.

El equivalente en Windows, podríamos decir que es wget, vamos a ver sus características y utilidades.

4.2.- CURL

- Qué hace el comando
 - Este comando se puede utilizar tanto en Linux, Windows y Mac
 - Lo podemos utilizar para:

- Ejemplo: curl -O http://google.es/test.es -O <http://google.es/test2>
- Utilización del comando curl para conocer las cookies que se descargan.
Sintaxis: curl --cookie-jar nombreArchiv URL -O
 - Ejemplo: curl --cookie-jar Mycookies.txt https://www.amazon.es /index.html -O
- Descargar archivos de un FTP. Sintaxis curl -u username:password -O ftp://URL_ftp/nombreArchivo
 - Ejemplo: curl -u username:password -O ftp://ejemplo/test
- Restringir el ancho de banda. Sintaxis: curl --limit-rate Número_K URL/nombreArchivo -O
 - Ejemplo: curl --limit-rate 100K http://ejemplo.es/test -O
- Por qué responde a la pregunta
 - A través del comando CURL podemos acceder a varios servicios de un servidor tales como que nos muestre el contenido de una página, descargar archivos o contenido, etc. Si este nos responde y nos permite la descarga o nos envía la información solicitada, significa que podemos acceder a él y está disponible.

5.- ¿Qué otros comandos te han hecho falta?

No he utilizado todos los comandos abajo descritos, pero a nivel general creo que son unos de los más importantes que debemos conocer:

Comando	Descripción
Cd	Muestra el directorio actual y permite cambiar a otros directorios. Con el parámetro /D más la unidad y la ruta también puede cambiarse la unidad. Mediante cd.. puede cambiarse al directorio superior.
Chdir	Muestra el directorio actual y permite cambiar a otros directorios. Con el parámetro /D más la unidad y la ruta también se puede cambiar la unidad. Mediante chdir puede cambiarse al directorio superior (tiene la misma función que cd).
cls	Elimina el contenido de la pantalla.
dir	Muestra todas las carpetas y archivos dentro del directorio actual. Puede restringirse la salida mediante atributos (/A), simplificar la lista (/B), o mostrar todos los subdirectorios y sus archivos (/S).
echo	Muestra un mensaje y es utilizado, sobre todo, en scripts y archivos batch.

mkdir	Crea un nuevo directorio en la ruta especificada. Si los directorios ya no existen en la ruta, mkdir los genera automáticamente. Alternativamente también puede utilizarse el comando md.
chkdsk	Revisa y repara (con el parámetro /R) un soporte de datos.