

Shell Commands Practical

7/02/22

Name - Rudraksh Karpe Branch - Computer Engineering

Roll No. - SCOB86

Aim - Explore and study of TCP/IP utilities and network

NETSTAT Command

- This command is used to get the networking stats of the computer on which the command is being used

```
netstat
```

```
→ /mnt netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State           I-Node    Path
/mnt netstat
```

Ifconfig command

- Using this command we can get the all the ip addresses connected to the computer

Step 1 :

```
sudo apt-get install net-tools
```

```
→ /mnt sudo apt-get install net-tools
[sudo] password for rudraksh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
net-tools is already the newest version (1.60+git20181103.0eebece-1).
0 upgraded, 0 newly installed, 0 to remove and 159 not upgraded.
```

Step 2 :

```
ifconfig
```

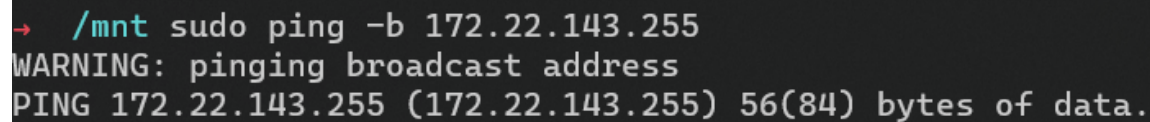
```
→ /mnt ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.22.134.108 netmask 255.255.240.0 broadcast 172.22.143.255
    inet6 fe80::215:5dff:fee6:33ae prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:e6:33:ae txqueuelen 1000 (Ethernet)
    RX packets 3017 bytes 567788 (554.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 113 bytes 7886 (7.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ping command

- Ping works by **sending an Internet Control Message Protocol (ICMP) Echo Request to a specified interface on the network and waiting for a reply**. When a ping command is issued, a ping signal is sent to a specified address. When the target host receives the echo request, it responds by sending an echo reply packet
- To run ping command pick any IP address from the ifconfig output and ping it

```
ping YOUR_IP_ADDRESS
```



```
→ /mnt sudo ping -b 172.22.143.255  
WARNING: pinging broadcast address  
PING 172.22.143.255 (172.22.143.255) 56(84) bytes of data.
```

Whois command

- In Linux, the whois command line utility is a **WHOIS client** for communicating with the WHOIS server (or database host) which listen to requests on the well-known port number 43, which stores and delivers database content in a human-readable format.
- To run the whois command download the following requirements

step 1:

```
sudo apt-get update -y
```

```
→ /mnt sudo apt-get update -y
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.6 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 Packages [17.9 MB]
Fetched 17.9 MB in 1min 4s (279 kB/s)
Reading package lists... Done
```

step 2:

```
sudo apt-get install -y whois
```

```
→ /mnt sudo apt-get install -y whois
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  whois
1 upgraded, 0 newly installed, 0 to remove and 158 not upgraded.
Need to get 81.1 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 whois amd64 5.5.11 [81.1 kB]
Fetched 81.1 kB in 12s (6,782 B/s)
(Reading database ... 22702 files and directories currently installed.)
Preparing to unpack ../whois_5.5.11_amd64.deb ...
Unpacking whois (5.5.11) over (5.5.9) ...
Setting up whois (5.5.11) ...
/mnt |
```

- Now you can run whois command

```
whois
```

```

→ /mnt whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-I                      query whois.iana.org and follow its referral
-H                      hide legal disclaimers
    --verbose           explain what is being done
    --no-recursion      disable recursion from registry to registrar servers
    --help              display this help and exit
    --version           output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                find the one level less specific match
-L                find all levels less specific matches
-m                find all one level more specific matches
-M                find all levels of more specific matches
-c                find the smallest match containing a mnt-irt attribute
-x                exact match
-b                return brief IP address ranges with abuse contact
-B                turn off object filtering (show email addresses)
-G                turn off grouping of associated objects
-d                return DNS reverse delegation objects too
-i ATTR[,ATTR]... do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE]... only look for objects of TYPE
-K                only primary keys are returned
-r                turn off recursive look-ups for contact information
-R                force to show local copy of the domain object even
                  if it contains referral
-a                also search all the mirrored databases
-s SOURCE[,SOURCE]... search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST find updates from SOURCE from serial FIRST to LAST
-t TYPE           request template for object of TYPE
-v TYPE           request verbose template for object of TYPE
-q [version|sources|types] query specified server info

```

Tracing command

- The **tracert** command is a **command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.**

Step 1:

```
sudo apt install pvm-dev
```



```

➤ /mnt sudo apt install pvm-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config fonts-dejavu-core libc-dev-bin libc-devtools libc6-dev libcrypt-dev libcrypt1 libdeflate0 libfontconfig1 libfreetype6 libgd3 libjbig0
  libjpeg62-turbo libncurses-dev libncurses6 libncursesw6 libnsl-dev libpam0g libpng16-16 libpvm3 libreadline-dev libreadline8 libtiff5 libtinfo6
  libtirpc-common libtirpc-dev libtirpc3 libwebp6 libxpm4 linux-libc-dev manpages manpages-dev ncurses-bin pvm rpcsvc-proto ucf
Suggested packages:
  glibc-doc libgd-tools ncurses-doc libpam-doc readline-doc man-browser
Recommended packages:
  libgpm2
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core libc-dev-bin libc-devtools libc6-dev libcrypt-dev libdeflate0 libfontconfig1 libfreetype6 libgd3 libjbig0
  libjpeg62-turbo libncurses-dev libnsl-dev libpng16-16 libpvm3 libreadline-dev libtiff5 libtirpc-dev libwebp6 libxpm4 linux-libc-dev manpages
  manpages-dev pvm pvm-dev rpcsvc-proto ucf
The following packages will be upgraded:
  libcrypt1 libncurses6 libncursesw6 libpam0g libreadline8 libtinfo6 libtirpc-common libtirpc3 ncurses-bin
9 upgraded, 28 newly installed, 0 to remove and 149 not upgraded.
Need to get 15.1 MB of archives.
After this operation, 42.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

- Press Y to say Yes

```

glibc-doc libgd-tools ncurses-doc libpam-doc readline-doc man-browser
Recommended packages:
  libgpm2
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core libc-dev-bin libc-devtools libc6-dev libcrypt-dev libdeflate0 libfontconfig1 libfreetype6 libgd3 libjbig0
  libjpeg62-turbo libncurses-dev libnsl-dev libpng16-16 libpvm3 libreadline-dev libtiff5 libtirpc-dev libwebp6 libxpm4 linux-libc-dev manpages
  manpages-dev pvm pvm-dev rpcsvc-proto ucf
The following packages will be upgraded:
  libcrypt1 libncurses6 libncursesw6 libpam0g libreadline8 libtinfo6 libtirpc-common libtirpc3 ncurses-bin
9 upgraded, 28 newly installed, 0 to remove and 149 not upgraded.
Need to get 15.1 MB of archives.
After this operation, 42.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 libncurses6 amd64 6.3-2 [102 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main amd64 libncursesw6 amd64 6.3-2 [133 kB]
Get:3 http://ftp.harukasan.org/kali kali-rolling/main amd64 libtinfo6 amd64 6.3-2 [349 kB]
Get:4 http://ftp.harukasan.org/kali kali-rolling/main amd64 ncurses-bin amd64 6.3-2 [439 kB]
Get:5 http://ftp.harukasan.org/kali kali-rolling/main amd64 libpam0g amd64 1.4.0-11 [130 kB]
Get:6 http://ftp.harukasan.org/kali kali-rolling/main amd64 libcrypt1 amd64 1:4.4.27-1.1 [89.0 kB]
Get:7 http://ftp.harukasan.org/kali kali-rolling/main amd64 libtirpc-common all 1.3.2-2 [13.8 kB]
Get:8 http://ftp.harukasan.org/kali kali-rolling/main amd64 libtirpc3 amd64 1.3.2-2 [83.9 kB]
Get:9 http://ftp.harukasan.org/kali kali-rolling/main amd64 libreadline8 amd64 8.1.2-1 [168 kB]
Get:10 http://ftp.harukasan.org/kali kali-rolling/main amd64 manpages all 5.10-1 [1,412 kB]
Get:11 http://ftp.harukasan.org/kali kali-rolling/main amd64 ucf all 3.0043 [74.0 kB]
Get:12 http://ftp.harukasan.org/kali kali-rolling/main amd64 fonts-dejavu-core all 2.37-2 [1,069 kB]
Get:13 http://ftp.harukasan.org/kali kali-rolling/main amd64 fontconfig-config all 2.13.1-4.3 [281 kB]
Get:14 http://ftp.harukasan.org/kali kali-rolling/main amd64 libc-dev-bin amd64 2.33-1 [242 kB]
Get:15 http://ftp.harukasan.org/kali kali-rolling/main amd64 libpng16-16 amd64 1.6.37-3 [294 kB]
Get:16 http://ftp.harukasan.org/kali kali-rolling/main amd64 libfreetype6 amd64 2.11.1+dfsg-1 [400 kB]
Get:17 http://ftp.harukasan.org/kali kali-rolling/main amd64 libfontconfig1 amd64 2.13.1-4.3 [350 kB]
Get:18 http://ftp.harukasan.org/kali kali-rolling/main amd64 libjpeg62-turbo amd64 1:2.1.2-1 [164 kB]
Get:19 http://ftp.harukasan.org/kali kali-rolling/main amd64 libdeflate0 amd64 1.8-1 [53.1 kB]
Get:20 http://ftp.harukasan.org/kali kali-rolling/main amd64 libjbig0 amd64 2.1-3.1+b2 [31.0 kB]
Get:21 http://ftp.harukasan.org/kali kali-rolling/main amd64 libwebp6 amd64 0.6.1-2.1 [258 kB]
Get:22 http://ftp.harukasan.org/kali kali-rolling/main amd64 libtiff5 amd64 4.3.0-3 [295 kB]
Get:23 http://ftp.harukasan.org/kali kali-rolling/main amd64 libxpm4 amd64 1:3.5.12-1 [49.1 kB]
Get:24 http://ftp.harukasan.org/kali kali-rolling/main amd64 libgd3 amd64 2.3.0-2 [137 kB]
Get:25 http://ftp.harukasan.org/kali kali-rolling/main amd64 libc-devtools amd64 2.33-1 [250 kB]
Get:26 http://ftp.harukasan.org/kali kali-rolling/main amd64 linux-libc-dev amd64 5.15.15-2kali1 [2,202 kB]
53% [26 linux-libc-dev 592 kB/2,202 kB 27%]
361 kB/s 21s

```

Step 2:

tracer

- Now you can run trace command accordingly

```

→ /mnt tracer
libpvm [pid1058] /tmp/pvmd.1000: No such file or directory
libpvm [pid1058] /tmp/pvmd.1000: No such file or directory
libpvm [pid1058] /tmp/pvmd.1000: No such file or directory
libpvm [pid1058]: pvm_mytid(): Can't contact local daemon
libpvm [pid1058]: Error Joining PVM: Can't contact local daemon
→ /mnt

```

ARP Command

- arp command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. ARP stands for **Address Resolution Protocol**. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).

```
arp
```

```

→ /mnt arp
Address      HWtype  HWaddress      Flags Mask    Iface
WAR-WACHINE.mshome.net ether    00:15:5d:e6:3c:08 C             eth0

```