1.B NETWORKING COMMANDS

VNStat

It is one of the most complete network commands. It works on all Linux and BSD systems, and allows us to monitor network traffic from the console.

- Installation is simple and fairly quick, allowing monitoring of all network interfaces.
- With VNStat we can collect all traffic needed from any configured interface.
- One of the big differences between VNStat and other tools is that VNStat collects kernel data instead of the interface itself, which means a lighter execution for the system.
- It will not require administrator permissions to run.
- It has the ability to store gathered information so your information never goes missing, even if the system crashes or reboots itself.
- You can set Vnstat to listen to traffic, daily or by billing period, as well as many other options.
- It stands out for its flexibility when configuring the reading of traffic.
- Finally, it is possible to set Vnstat output to generate console graphics and even customize them with colours.

Ping (Unix/Windows)

Ping dates from the 70s and is known for being one of the most basic network commands. However, it is not as simple as we believe and has many more uses than those we already know. It is based on the ICMP protocol and is used to determine:

- If there is connectivity between your machine and another machine on the network.
- It's used to measure the "speed" or latency time.

It is a command that exists on all operating systems that support TCP/IP, and it is a basic command that you should know.

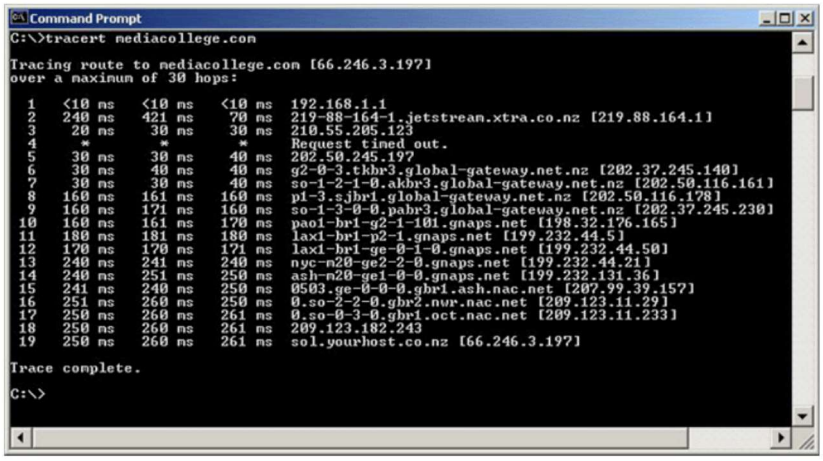
Ping is known for having dozens of parameters and the one that we find more useful is the one responsible for monitoring “the number of packages to send.” There are networks that undo the first package, so it is essential to send at least three so we can check that at least one has arrived without being discarded. For this, we use the -c parameter.

The same technique can be used to determine the loss percentage of packages in our network, sending ten packages and seeing if any gets lost. The number of packages that usually get lost in the network will surprise you. (This tool is included in Pandora FMS)

Execution: Ping name/System IP

Traceroute (Unix/Windows)

The main objective of this tool is to know the traveling path of a package through our network. This network command will tell us where the package is going through (machines, switches, routers) and check that our network is working properly. If you encounter any problems, it will allow us to have a rough idea about where the fault lies.



Execution:

traceroute –n (on Unix / Linux)

tracert –d (on Windows)

Arp (Unix/Windows)

This network command is used to change and view the ARP table, which contains the mappings between the IP address and the MAC address. It only sees the connections in our local area network segment (LAN), so it could be called "low level". However, it's used to discover what machines are directly connected to our host or what machines we are connected to. It is a diagnostic tool, and sometimes it can be interesting to monitor it in order to discard ARP Poisoning attacks, which are one of the most common forms of phishing attacks in local networks.

Execution: arp –a

Curl and wget (Unix/ Windows)

These are essential commands to do HTTP, HTTPS or FTP requests to remote servers. It allows you to download files or whole web pages, even recursively (it literally allows us to make a "copy" of a website, including images). It supports cookies and allows you to send POST requests, in addition to "simulate a" user agent, use a http proxy or even a SOCKS4/5 proxy.

One of the most common utilities in integration with Pandora FMS, is to verify the contents of a specific web page. Because wget / curl allows us to download the entire contents of a web, it is easy to compare the MD5 of that content with a value previously verified. If it changes, it means that the Web has been altered.

Netstat (Unix/Windows)

Network command identifies all TCP connections and UDP open on a machine. Besides this, it allows us to know the following information:

- Routing tables to meet our network interfaces and its outputs.
- Ethernet statistics that show sent and received packages and possible errors.
- To know the id of the process that is being used by the connection.
- Netstat is another basic command as Ping that meets many elementary functions.

Whois (Unix/ Windows)

This network command is used to query data domains: to find out who owns the domain, when that domain expires, to view the configured logs, contact details, etc. Its use is

highly recommended to contact the administrators of the domains or when incidents of migration of services such as mail and web happen.

To use 'whois' on Windows you need to download the software from this url: https://technet.microsoft.com/en-us/sysinternals/whois.aspx

SSH (Unix/Linux/Windows)

Command to run terminals on remote machines safely. SSH allows any user to run a console just by registering and entering his credentials. So you can run the commands you want as if you were in local.

More details you need to know about SSH:

Putty is recommended when using SSH in Windows. You can find it here: http://www.putty.org/

- To enable a remote computer to connect to our server via SSH, an SSH server must be installed and set up as FreeSSHd.
- SSH also allows to obtain an interactive remote Shell, execute remote commands and copy files in both directions.
- SSH is the natural replacement of classic tools like Telnet or FTP, and has become a basic tool in the administration of systems over the years. It is extremely powerful despite its complex combinations of symmetric encryption and authentication schemes, and verification, and it is the target of continuous attacks.

TCPDump (Unix/Linux/Windows)

It is one of the "basic" tools of network commands, and when used right, goes on to become a great ally for network administrators, system administrators or programmers.

TCPDump is an advanced command used to inspect traffic from different interfaces of a machine so you can get the exchanged packages. You can dump output to file so then you can analyse it with more powerful sniffers and graphical interfaces such as Wireshark. For Windows, you must use WinDump.

Ngrep (Unix/Linux/Windows)

- The grep command power is taken to the network.

- It is a TCPDump with a substring text filter in real time.
- It has a very powerful filtering system for regular expressions and it is typically used to process files generated by tcpdump, wireshark, etc.
- It is a communication package filter over HTTP, SMTP, FTP, DNS and other protocols.

NMAP (Unix/Windows)

NMAP is considered the father of the general network scanners. Although today there are more reliable tools for some tasks (like Fping), NMAP is a very versatile tool for scanning networks. It is used to determine which hosts are alive in a network and to do different ways of scanning.

Netcat (Windows/Unix)

NetCat, or NC, is the network command most versatile that exists nowadays and one of the lightest. However, its use requires some imagination. Only if you've played with scripting, you will understand the subtlety of its name: NetCat. It is a tool designed to be used as a destination of a redirect (one pipe or |). It is used to send or receive information about a connection. For example, a WEB request to service would be something as simple as:

echo -e "GET http://pandorafms.com HTTP/1.0\n\n" | nc pandorafms.com 80

Lsof (Unix/Windows)

The 'lsof' command is not only used as a network tool, but also is used to identify which files have an open process. In Unix environments, a file can be a network connection, so that is used to know which ports have an open particular running process, something extremely useful in specific cases.

IPtraf (Linux)

Special command to obtain traffic statistics. It has a ncurses interface (text) to analyze real-time traffic passing through an interface. It allows you to work at low-level and to see what pairs of connections are established on each machine, and to see in detail the traffic connection of every pair, all in real-time.