Section 20 – Network Analysis and Troubleshooting

Questions

Please read the following questions carefully and try to answer them. You will find the correct answers, with an explanation where necessary, in the Answers.pdf file located in the same folder

1. The PING command can be used to troubleshoot the following (choose all that apply):
    a. Network connectivity
    b. DNS resolve
    c. Network speed
    d. The number of hops till the remote host
2. Using a larger MTU size in PING requests can help diagnose network fragmentation problems due to congestion (for example)
    a. True
    b. False
3. In order for it to work, traceroute sends a number of packets with a TTL of 1. It increases the TTL of the packets on each subsequent request until the TTL finally equals the total number of hops
    a. True
    b. False
4. When a star is returned in the time field of traceroute answer, this may be a result of: (choose all that apply)
    a. The gateway did not respond until the request timed out
    b. The host is discarding expired packets
    c. A firewall is blocking those packets
    d. The host may be down
5. When you want to display basic information about the network cards installed on the server, you use netstat with the following argument:
    a. –i
    b. –a
    c. –l
    d. –n
6. When netstat is invoked without any arguments, the following output is displayed:
    a. The total number of connections (both listening and in established)
    b. The listening ports
    c. The ESTABLISHED connections
    d. The network bandwidth

7. In order to display both the active connections and the listening ones, you use netstat with the following arguments:
    a. –i
    b. –n
    c. –a
    d. –l
8. When you want netstat to ignore resolving ports to service names you can use the following argument:
    a. –n
    b. –l
    c. –p
    d. –a
9. When connections are in TIME_WAIT state that means:
    a. They are starting to communicate
    b. They are in the process of closing
    c. The remote host did not reply
    d. None of the above
10. When the TCP state is SYN_SENT this means:
    a. Connections are closing
    b. Connections are starting
    c. The machine cannot handle that number of connections and it may need some kernel tuning
    d. None of the above
11. When you want to display the current routing table on the machine you use netstat with the following argument:
    a. –a
    b. –l
    c. –p
    d. –r
12. What happens when a machine does not have a default gateway? (choose all that apply)
    a. It cannot connect to any hosts outside its local subnet
    b. No hosts can connect to it from outside the current subnet
    c. The network cards will not function correctly
    d. None of the above
13. On Linux, you can use netstat to capture network activity for a specific period of time
    a. True
    b. False
14. Tcpdump and Wireshark are examples of network sniffers
    a. True
    b. False
15. Using tcpdump, when you want to capture packets on NIC eth0, you'd use it like this:
    a. tcpdump –p eth0
    b. tcpdump –i eth0
    c. tcpdump –r eth0

    d. tcpdump eth0

16. When you want to save tcpdump date to a file instead of displaying it to the standard output, you’d use the following switch
    a. –s
    b. –w
    c. --file
    d. none of the above
17. When you want to read tcpdump data in ASCII format, you’d use the following switch:
    a. –A
    b. –r
    c. –w
    d. –i
18. To read tcpdump data from a file you use the following argument
    a. –A
    b. –r
    c. –w
    d. –i
19. The tcpdump command stores packet information in libpcap format, which makes the data readable by other applications that use the same format like Wireshark
    a. True
    b. False
20. In order to sniff packets that are not intended to the received by the current host, the NOC must operate in promiscuous mode
    a. True
    b. false