Universidade do Algarve WireShark - Capturing Packets 2024

Lab #3

YourName Turma YourStudentNumber

Completely fill the circles as shown: ○○●○

Q1 A new analyst has just joined a company and can't seem to see any packets coming through on Wireshark. What should be done to help the analyst?

● Add the analyst to the Wireshark permissions group (access control).
○ Have the analyst install Wireshark.
○ Have the analyst run Wireshark as sudo.
○ Have the analyst log in as root.

Q2 A team member is looking to capture traffic on the server. The team member says the traffic is visible, but the capture file cannot be saved. Which is a likely solution?

● Stop capturing.
○ Start capturing.
○ Select the correct network.
○ Close the capture file.

Q3 A colleague is working on observing only HTTPS packets from an existing file. Which filter should be used?

○ Display filter with http.
○ Capture filter with tcp.port==443.
● Display filter with tcp.port==443.
○ Capture filter with http.

Q4 An analyst has been alerted of strange network activity coming from IP address 18.160.96.85 and has been tasked with locating all the packets containing the IP address in Wireshark capture. Which filter should be used?

○ ip.addr=18.160.96.85
○ ip.src==18.160.96.85
○ ip.dst==18.160.96.85
● ip.addr==18.160.96.85

Q5 A server has a lot of traffic on a particular IP address. To observe other packets, the analyst just wants to see those packets not associated with IP address 18.160.96.85. Which filter should be used?

○ !(ip.addr=18.160.96.85) or tcp.port==443
○ (ip.addr!=18.160.96.85) or tcp.port==443
● !(ip.addr==18.160.96.85) and (tcp.port==443 or tcp.port==80)
○ (ip.addr!=18.160.96.85) and tcp.port==80