Free Questions for CS0-003 by go4braindumps

Shared by Miranda on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A grep [IP address] packets.pcap

B cat packets.pcap | grep [IP Address]

Options:

C) tcpdump -n -r packets.pcap host [IP address]

D) strings packets.pcap | grep [IP Address]

Answer:

C

Explanation:

tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official Reference:

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_studied/

Question 2

Question Type: **MultipleChoice**

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

A grep [IP address] packets.pcap

B cat packets.pcap | grep [IP Address]

Options:

C) tcpdump -n -r packets.pcap host [IP address]

D) strings packets.pcap | grep [IP Address]

Answer:

C

Explanation:

tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official Reference:

https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_studied/