210-255$^{\text{Q\&As}}$

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

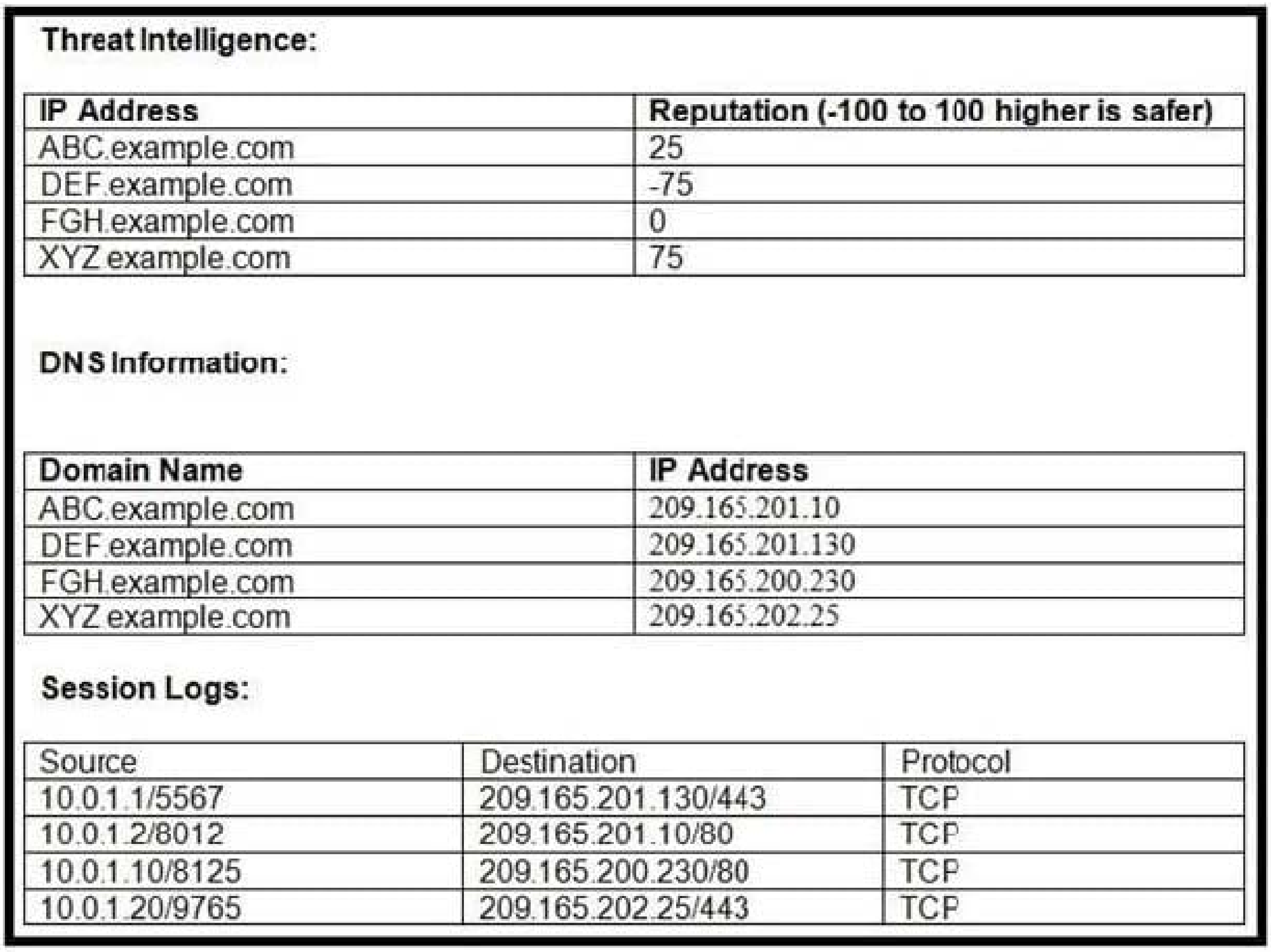
https://www.pass4itsure.com/210-255.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Refer to the exhibit.



Threat Intelligence:

IP Address	Reputation (-100 to 100 higher is safer)
ABC.example.com	25
DEF.example.com	-75
FGH.example.com	0
XYZ.example.com	75

DNS Information:

Domain Name	IP Address
ABC.example.com	209.165.201.10
DEF.example.com	209.165.201.130
FGH.example.com	209.165.200.230
XYZ.example.com	209.165.202.25

Session Logs:

Source	Destination	Protocol
10.0.1.1/5567	209.165.201.130/443	TCP
10.0.1.2/8012	209.165.201.10/80	TCP
10.0.1.10/8125	209.165.200.230/80	TCP
10.0.1.20/9765	209.165.202.25/443	TCP

Which host is likely connecting to a malicious site?

A. 10.0.1.10

B. 10.0.1.1

C. 10.0.1.2

D. 10.0.1.20

Correct Answer: B

QUESTION 2

Which two useful pieces of information can be collected from the IPv4 protocol header? (Choose two.)

A. UDP port which the traffic is destined

B. source IP address of the packet

C. UDP port from which the traffic is sourced

D. TCP port from which the traffic was source

E. destination IP address of the packet

Correct Answer: BE

QUESTION 3

Which feature is used to find possible vulnerable services running on a server?

A. CPU utilization

B. security policy

C. temporary internet files

D. listening ports

Correct Answer: D

QUESTION 4

Where do you navigate in Wireshark to download files?

A. File > Export text

B. File > Export Binaries

C. File > Export Files

D. File > Export Objects

Correct Answer: D

QUESTION 5

Which of the following is not true regarding the use of digital evidence?

A. Digital forensics evidence provides implications and extrapolations that may assist in proving some key fact of the case.

B. Digital evidence helps legal teams and the court develop reliable hypotheses or theories as to the committer of the crime or threat actor.

C. The reliability of the digital evidence is vital to supporting or refuting any hypothesis put forward, including the attribution of threat actors.

D. The reliability of the digital evidence is not as important as someone\\'s testimony to supporting or refuting any hypothesis put forward, including the attribution of threat actors.

Correct Answer: D